This research study is available online at the ECAR Web site (www.educause.edu/ecar). The content of this study is restricted to authorized ECAR subscribers and to those who have separately purchased this study. The username and password below are required to gain access to the online version and are to be used only by those who may legally access the content.

Username: ERS0305
Password: SECURITY924
Information Technology Security: Governance, Strategy, and Practice in Higher Education
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

Copyright 2003 EDUCAUSE. All rights reserved. This ECAR research study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR research studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to ecar@educause.edu.
## Contents

**Foreword**  ................................................................. 5  
ECAR background • IT security in higher education • Important contributions

**Chapter 1**  Executive Summary ................................................................. 9  
Methodology and participants • Key findings • Conclusion

**Chapter 2**  Introduction ................................................................. 19  
Definition of information security • Establishing requirements • How IT security is different in higher education • Need for further research

**Chapter 3**  Methodology and Participant Demographics  ..................... 31  
Research approach • Characteristics of responding institutions • Position and experience of individuals responding

**Chapter 4**  IT Security Technologies Implemented by Higher Education Institutions ........ 39  
Firewalls • Data protection strategies • Remote network access • Wireless security • Authentication and access control • Antivirus protection • Strategies to reduce vulnerability

**Chapter 5**  Organization, Leadership, Policies, and Awareness ............... 59  
IT security on campus • Staffing • Security organization • Security policy • Leadership in policy development • Awareness • Budget

**Chapter 6**  IT Security Planning and Practice ............................................. 87  
Security planning • Risk assessments and audits • Maintaining systems • Controlling access • Detection and monitoring

**Chapter 7**  IT Security Incidents, Response Practices, and Procedures ........ 97  
Security Incidents • Incident handling procedures • Individuals involved in responding to incidents • Reporting incidents to senior management

**Chapter 8**  IT Security Program Success: What Matters  .......................... 109  
Assessing success • Factors that influence success • Barriers to IT security
Chapter 9  Effective Practices and Lessons Learned .............................................. 121
Not just about technology • Engagement of senior leaders • Effective planning
• Monitoring • Working with constituents • New incentives • Differences of opinion

Chapter 10  Present and Future Alignment of Security Practices ......................... 131
IT security beliefs in higher education • Aligning IT security with institutional
needs • Changing IT security environment • Future trends • Conclusion

Appendix A  Interviewees in Qualitative Research ............................................. 149

Appendix B  Institutional Respondents to the Online Survey ............................ 153

Appendix C  Glossary ......................................................................................... 159

Appendix D  Bibliography ................................................................................ 169
The EDUCAUSE Center for Applied Research (ECAR) was launched on January 1, 2002, to create a body of research and analysis on important issues at the intersection of higher education and information technology. ECAR is fulfilling its mission through a program of symposia and through the publication of
- biweekly research bulletins oriented to senior campus functional executives;
- detailed studies designed to identify trends, directions, and practices in an analytically robust fashion; and
- case studies designed to showcase campus activities and highlight effective practices, lessons learned, and other insights from the practical experience of campus leaders.

Since ECAR’s inception, two symposia have been held and close to 60 research publications have been issued.

IT Security in Higher Education

For well over four decades, providing secure IT services to their constituents has been a top priority for college and university administrators. Institutions have invested money and human resources to protect their information assets and those of faculty and students. With no end in sight to security threats and breaches, their efforts are growing. Rapidly increasing bandwidth demands, the evolution of distributed computing architectures (and governance), and an incredible rise in computer crimes place increasing stresses on higher education’s institutions and their computing infrastructures. Even institutions famous for their IT security investments and policies are at risk and have suffered newsworthy break-ins, resulting in the theft of student Social Security numbers, medical records, and other confidential information. Colleges and universities have also been the launch pads for numerous virus and denial-of-service attacks in recent years, creating high public relations, financial, and regulatory problems for higher education as a whole.

EDUCAUSE efforts in this arena have been noteworthy. EDUCAUSE has long been recognized as a major participant in national efforts to secure higher education’s communications and computing infrastructure. It has participated with Internet2 to conceive, develop, and deploy technologies, techniques, and standards that enhance identity services and other middleware elements essential to IT security. We especially commend the work of the EDUCAUSE/Internet2 Computer and Network Security Task Force. Mark Bruhn of Indiana University, Ken Klingenstein of Inter-
net2, Mark Luker and Rodney Petersen of EDUCAUSE, Dan Updegrove of The University of Texas at Austin, and Gordon Wishon of the University of Notre Dame deserve particular attention and thanks. In addition to helping secure higher education, these busy people advised us throughout this research. Of course they bear no responsibility for our findings or conclusions. This study’s authors also owe thanks to EDUCAUSE for data from the 2002 EDUCAUSE Core Data Service survey.

The EDUCAUSE/Internet2 Computer and Network Security Task Force has identified several issues for further study. These include making IT security a higher and more visible priority in higher education; doing a better job with existing security tools by, for example, revising institutional policies; and designing, developing, and deploying improved security for future research and education networks. In the spirit of the Bush administration’s national security goals, the task force is working to raise the level of security collaboration among higher education, industry, and government, and to integrate higher education work on security into the broader national effort to strengthen critical infrastructure.

Despite the national attention and ongoing efforts of EDUCAUSE, Internet2, and other organizations to develop and foster a modern and secure IT infrastructure in higher education, our knowledge of the current state and future plans of colleges and universities vis-à-vis IT security has been largely anecdotal to this point. Leadership is purported to be reactive rather than proactive, with a lack of clearly defined goals. Similarly, the academic culture often finds the goals of security, academic freedom, and intellectual freedom to be antithetical.

This ECAR study is designed to provide a fact-based and national perspective of higher education’s security environment that can lead to the improvement of institutions’ cybersecurity. It establishes a security baseline for higher education. It identifies what security policies, tools, and procedures are currently in place. Institutions will be able to compare their own investments and practices with those of similar institutions. Emphasis is placed on both the benefits and risks of implementing security solutions, including trade-offs and future trends.

**Important Contributions**

ECAR research studies are the result of a team effort. Robert B. Kvavik, ECAR senior fellow and professor at the University of Minnesota, and John Voloudakis, CTO of Cap Gemini Ernst & Young’s (CGE&Y) Higher Education Practice, authored this report. Their intellectual leadership is evident in the work itself. Their work was fostered by Judith Caruso, ECAR fellow and director of policy, security, and planning at the University of Wisconsin–Madison, who managed the research project, authored the executive summary, and coauthored the case study of IT security at Indiana University. Judith Pirani led the design, execution, and analysis of this study’s qualitative aspects, adding a richness and texture that survey data alone can rarely supply. Former ECAR Fellow Paula King was instrumental in the creation and deployment of the quantitative survey whose results form the backbone of this study and supported the University of Washington case study. Robert Albrecht coauthored the case study of IT security at Indiana University and provided thoughtful commentary on drafts and research design throughout this project.

Of course, the real team in any ECAR study is the EDUCAUSE community. Our ability to develop a good understanding of practices, policies, and directions in higher education depends on our associates’ goodwill. Hundreds of busy CIOs and security officers shared their experiences and expertise.
on our quantitative survey, and dozens more generously gave their time in interviews. Jim Bruce of MIT, Ron Johnson of the University of Washington, and Michael McRobbie of Indiana University gave our researchers access to their staff for intensive discussions during on-site case visits. We cannot thank them enough.

The EDUCAUSE staff is also part of our community, and our ability to conduct this research depends on their provision of a myriad of services big and small. The EDUCAUSE team is always there when you need them, and their commitment to excellence is evident in all that they do. Thank you.

Finally, ECAR, while now enjoying the support of more than 200 college and university subscribers, continues to depend on the generous support of a small and dedicated cadre of corporate sponsors. Cap Gemini Ernst & Young, Collegis, Datatel, Hewlett-Packard, Microsoft, PeopleSoft, SCT, and WebCT not only provide direct financial support but are also generous with their advice and skilled resources. John Voloudakis of CGE&Y, for example, coauthored this report and was instrumental to the project.

This study reminds us that the opportunities and challenges posed by networked information demand responses that are at once technological and cultural in nature. The story of IT security in higher education is ultimately a story of people—people on the outside and inside of our academies who may have sinister motives, and people on the outside and inside with good intentions but incomplete knowledge of or attention to good practice. These people, good and bad, converge in, on, and around our virtual Commons, which we have optimized to facilitate communication and the free exchange of scholarly ideas. In the end, higher education's potential to secure its stakeholders and their information assets will depend on our IT leaders' creativity, vigilance, investment, and technical sophistication on the one hand and on communication, education, awareness training, and collaboration among institutional subunits on the other. IT security, it seems, is everyone's responsibility.

Richard N. Katz
Executive Summary

Providing sound information technology (IT) security at colleges and universities is essential to protecting information assets, safeguarding the integrity of institutional processes, and ensuring compliance with state and federal regulations. One challenging characteristic of higher education is a culture that values relatively unfettered and timely access to information and the free and continuous scholarly exchange of ideas. This culture requires that a secure environment carefully balance the extremes of leaving institutional and faculty information assets unprotected in a misplaced spirit of academic laissez faire, and choking off critical pathways of scholarly exchange by controlling access to these assets too tightly.

The advent of the World Wide Web in 1993 and its commercialization and globalization in the mid-1990s heightened the importance of protecting institutional infrastructure and intellectual assets. Recent legislation such as the Health Insurance Portability and Accountability Act (HIPAA), the Digital Millennium Copyright Act, and the Gramm-Leach-Bliley Act has imposed additional security requirements on higher education. Successful security efforts require not only increased investments in technologies, policies, software, and personnel but also the time and attention of all students, faculty, and staff.

Despite this heightened attention, very little is known about the current state and future plans of IT security at colleges and universities. This study was undertaken, then, to investigate the state of IT security practices and investments in higher education and to compare and contrast the practices and investments, where possible, with those in other industries.

For this study, information security is defined as

- preserving confidentiality;
- protecting information from unauthorized use or disclosure;
- assuring information’s integrity, including the accuracy and completeness of the data, through protection from unauthorized, unanticipated, and unintentional modification; and
- making data available to authorized users on a timely basis.

Using the ISO/IEC 17799 framework for security standards as a guide, we designed this study to provide an analytical baseline of higher education’s security environment. This study identifies what security policies, tools, and procedures are currently in place and thus raises important policy and op-
erational questions that can constitute the basis for deeper analysis and research. With this study, institutions can begin to compare their investments and practices with those of similar institutions. This study also—within limits—lets us tentatively compare higher education’s practices with those in other industries, again suggesting areas for deeper inquiry and possible action.

**Methodology and Study Participants**

This study consisted of five data collection and analytical initiatives:

- a literature review to identify and clarify the study’s major elements and create a working set of hypotheses to be tested;
- consultation with a select group of IT security leaders in higher education to identify and validate the most interesting research questions and hypotheses that would frame the quantitative survey instrument;
- a quantitative survey of 435 higher education institutions;
- qualitative telephone interviews with 42 technology executives, managers, and faculty members at 18 institutions; and
- four in-depth case studies including institution studies of the Massachusetts Institute of Technology, the University of Indiana, and the University of Washington, and a study of the management procedures for press-reported security incidents at the Georgia Institute of Technology, the University of Montana, and The University of Texas at Austin.

The participants in the quantitative Web-based survey consisted of 414 U.S. and 21 Canadian institutions of which 57 percent are public. With a survey response rate of 30 percent from EDUCAUSE institutions, the responding schools mirror closely the EDUCAUSE membership by Carnegie class. In our data analysis we looked for factors that proved to be significant differentiators in IT security. Size of institution, whether measured by number of students, network users, or devices proved to be a significant variable, while Carnegie class did not. The survey respondents consisted largely of CIOs (42 percent), chief IT security officers (12 percent), and other IT staff (39.5 percent). Nearly one-half of the respondents (46 percent) had more than 10 years of experience with IT security.

**Key Findings**

Several IT security taxonomies guide our findings. The first looks at institutions in two dimensions: security technologies in use and the security culture—leadership, organization, values, and rules. Institutional investments in these areas result from

- perceptions about the risks facing the institution—internal, external, or both;
- the institution’s propensity to take or accept risks;
- the resources an institution has to deploy, both financial and human; and
- the institution’s priorities and culture reflecting where it feels it can effectively make changes.

**Firewalls**

Firewalls are a key technology in higher education. Of all technologies employed by survey respondents, firewalls were the most commonly used (87 percent), and another 10 percent are currently installing them. Carnegie class was a significant differentiator regarding perimeter firewall implementation. Eighty-three percent of the baccalaureate institutions have installed perimeter firewalls, while only 40 percent of the doctoral-extensive institutions have installed them. Terry Gray of the University of Washington explained why large institutions avoid perimeter firewalls: “Border
firewalls have some long-term negative consequences, such as encouraging people to tunnel all manner of applications through ports that are rarely blocked by firewalls. Instead, push security perimeters and policy definition as close to the organizations and computers to be protected as possible, and make sure all sensitive traffic is encrypted. This serves the reality of the large institution. A one-size-fits-all strategy is problematic for the research university."

But disagreement exists even among large institutions. Paul Howell, information systems security officer at the University of Michigan, stated, "If you can install [perimeter firewalls] and operate them correctly, they tend to be the key thing to go after because they tend to keep undesirable traffic from the Internet [from] washing up on your machines. [Such traffic] can cause a lot of headaches."

**SSL Technology**

The most significant difference in technology use among large versus small institutions was in the adoption of Secure Sockets Layer (SSL) for Web transactions. SSL, a commonly used protocol for securing Internet data exchange, is an integral part of most Web browsers and uses a public- and private-key encryption system, including the use of a digital certificate. More than 86 percent of large institutions employed SSL compared with just 66 percent of small institutions. Also, SSL was heavily used by all doctoral institutions.

**Security Technology Use in Higher Education Versus Industry**

In general, higher education employs security technologies less often than industry. For example, the 2003 CSI/FBI Computer Crime and Security Survey¹ found that 98 percent of industry respondents had installed firewalls, versus 87 percent in our higher education survey. In addition, 73 percent of the CSI/FBI respondents use intrusion detection tools, versus 43 percent of our survey respondents. The greatest contrast between industry and higher education technology security is in electronic signature use, with usage of 56 percent reported by industry in a survey conducted by Top Layer Networks² and just 7 percent reported in our survey. These findings need to be viewed cautiously, as they reflect results obtained from different surveys administered at different times, but they do suggest further study and discussion.

**Wireless Security**

Large institutions and doctoral institutions differ from master's, baccalaureate, associate's, and, to some degree, Canadian institutions in the use of strategies to secure wireless network access. For example, the latter four institution types more often used 128-bit wired equivalency privacy (WEP), extensible authentication protocol (EAP), and firewalls, whereas large and doctoral institutions more often used Internet Protocol virtual private network (IP VPN), Kerberos, and remote authentication dial-in user service (RADIUS). Little difference exists between public and private institutions. Overall, the most commonly used wireless security technology was firewall technology, with more than 57 percent of institutions reporting its use.

**Authentication**

All institutions responding to the survey reported using some form of authentication. In addition, 24 percent of the institutions use two forms of authentication, and 50 percent use three or more forms. The form of authentication used—multiple-use passwords, multilevel passwords, password/PIN combinations, Kerberos, and the like—
varies depending on the perceived sensitivity of the data being protected at the institution. Nineteen percent of the survey respondents had implemented a single-sign-on system, another 19 percent were currently implementing one, and 48 percent said they plan to implement such a system in the next two years.

Biometrics

Biometric authentication technologies are virtually nonexistent in higher education. When comparing biometric technology use between our higher education survey respondents and respondents to three industry surveys, we found a significant difference in adoption. In the 2003 CSI/FBI Computer Crime and Security Survey, 11 percent of the industry respondents had installed biometric tools. In our study, only 1 percent of the higher education institutions reported using biometric technologies.

Antivirus Protection

Ninety-seven percent of the surveyed institutions have installed antivirus protection on their operating systems, 90 percent on their application servers, 92 percent on their e-mail servers, and 88 percent on other servers. These figures compare favorably with industry respondents’ 99 percent reported use of antivirus software in the 2003 CSI/FBI Computer Crime and Security Survey. Many higher education institutions (68 percent) said they require that all institutionally owned systems have antivirus protection installed to connect to the network, but only 36 percent required it of noninstitutionally owned systems. This requirement was weakest at large and doctoral institutions. This may be explained by the diversity of systems prevalent at those institutions, where nonmainstream desktop systems may not have readily available antivirus solutions at competitive prices.

Security Management

According to our respondents, day-to-day IT security management is the responsibility of central IT organizations (96 percent), and directors of networking are most often in charge (31 percent), followed by chief IT security officers (29 percent) and CIOs (7 percent). The position of chief IT security officer has been created largely since 1994; more than 22 percent of the institutions report having this position. Reasons for creating the position, however, vary among the institutions and include:
- an enterprise resource planning system implementation at Yale University;
- government and regulatory issues at South Dakota State University;
- new technology leadership at Notre Dame University; and
- for the Maricopa Community Colleges, the September 11 disaster.

Most often these chief IT security officers report to the CIO (51 percent) or another vice president (13 percent). According to survey respondents, 54 (12 percent) of their IT security managers have formal IT security certification such as a Certified Information Systems Security Professional (CISSP) certificate or a Global Information Assurance Certificate (GIAC). Martin Fraser, professor and chair of the computer science department at Georgia State University, commented on the significance of certification: “From the faculty perspective, certification does help—it lends credence and authority that can get the attention of academic units better. [It is] training that is acknowledged.”

Security Staffing

In the recent EDUCAUSE Core Data Service survey, institutions reported on the size of their IT security staff. Doctoral institutions employ the largest security staff, with an average of 2.5 full-time staff; baccalaureate institutions average only 0.37
full-time staff. The number of full-time staff, however, is more closely linked to the number of devices on the network than to Carnegie class. As the number of network devices increases, the number of full-time staff increases, especially as the number of devices exceeds 10,000.

The existence and size of a dedicated security staff proved a significant factor when we analyzed how many survey respondents viewed their security programs as successful. Respondents employing full-time security staff viewed their security programs as more successful than those who did not have full-time security staff.

As would be expected, the organization of staffing for IT security varies greatly from campus to campus. The majority (57 percent) report that security staffing is spread across multiple functions, 22 percent report having a single dedicated staff member, and 11 percent report having more than one dedicated staff member. The tug between centralization and decentralization of security staff is common in large decentralized campuses.

**Security Policies**

Two hundred and thirty-five of the institutions surveyed (54 percent) indicated that they have formal institutional policies covering IT security. Of these, 19 percent also had interim policies or policies in progress. Ninety-nine percent of the institutions had implemented policies regarding appropriate use of institutional assets, whereas only 39 percent had security policies covering application development. The number of policies, their scope, and the policy development and enforcement processes are unique to each institution, with some institutions viewing policies as critical and others intentionally limiting the number of institution-level policies. All respondents, however, agreed on the importance of policies that are easy to read, accessible, enforced, comprehensive in scope, regularly updated, and consistent across the institution. Mark Bruhn, chief IT security and policy officer at Indiana University, emphasized, “We need and want the formal policies to exist, but we also need another format that makes them easier to read, less formal, and more narrative.”

**Policy Development Leadership**

The policy development literature encourages the active engagement of senior management, not simply executive support or endorsement. According to James Wright, president of Dartmouth College, “It is vital that decisions on policies and practices regarding security and related issues be carefully vetted, understood, and authorized by both the highest levels of the campus leadership and the representatives of the campus community.” Michael McRobbie, vice president of information technology and CIO of Indiana University, advised, “Get your president on your side. Get him to say security is important publicly.” The ECAR survey indicated that most institutions include the IT organization, the CIO, and a campus or faculty task force in IT security policy development. Policy development was least likely to involve state agencies, boards of trustees, and presidents.

**Security as Institutional Priority**

We asked if IT security was one of the top three IT issues confronting higher education institutions today. Seventy-five percent of respondents agreed or strongly agreed, while only 10 percent disagreed or strongly disagreed. The respondents who strongly agreed were most likely to come from large doctoral institutions. When asked if IT security was a priority at their institutions, however, only 61 percent agreed or strongly
agreed. The gap between security as a top issue confronting the institutions (75 percent) and security as a priority (61 percent) raises some concerns. As with other risk-management activities, most people view IT security as a behind-the-scenes activity, and institutional leaders often attend to it only when a costly or embarrassing breach occurs.

Security Awareness

Surprisingly, only 33 percent of the institutions in our study had a formal security awareness program for students and faculty. A formal awareness program for staff was only slightly higher, at 39 percent for all institutions. Doctoral institutions were more likely to have awareness programs than other institutions. Some institutions include security awareness education as part of their student orientation. These percentages are disappointing, as this is one area where an increased expenditure and effort could have an enormous payback to the institution.

Resources

Obtaining adequate financial and human resources for IT security is a challenge for higher education institutions. When queried about the percentage of the total IT budget spent on security, 50 percent of the respondents reported that the budget for security represented 1 to 5 percent of the total central IT budget. When asked whether these resources were adequate, 44 percent disagreed or strongly disagreed. The reported security spending by higher education in our study is significantly less proportionately than that reported by government, banking, telecommunications, and other industries. According to Information Week’s 2002 Global Information Security Survey, respondents spent on average 12.4 percent of their overall IT budget on IT security.

Security Planning

Comprehensive IT security plans exist in almost 13 percent of the higher education institutions responding to our survey. Another 78 percent report that they either have a partial plan in place or are currently developing a plan. Small institutions are less likely than large institutions to have an IT security plan. Institutions with dedicated security staff are more likely to have a plan than those without dedicated staff.

Risk Assessment and Audit

Risk assessments help institutions evaluate the potential harm to their business should a security failure cause a loss of confidentiality, integrity, or information availability. Yet only 30 percent of higher education institutions responding to the survey have conducted such an assessment. Also, when asked about regular audits of enterprise systems and router configurations, 46 percent of the institutions reported that they audited on an irregular basis or not at all. These numbers appear to be low, indicating a need for both deeper research and greater attention to work in this security area.

Security Exposure Practices

All computers connected to a campus network present potential security exposures to the institution. This is an area where most institutions have good practices in place. In our study, 62 percent of institutions agreed or strongly agreed that they required all campus-owned computers connected to the network to have known security holes fixed. Fifty-nine percent agreed or strongly agreed that their institutions conduct regular and frequent scans to detect known security exposures in critical systems, but only 40 percent agreed or strongly agreed that their institutions conduct regular and frequent scans to detect known security exposures.
in all campus-owned computers connected to the network. Clearly, exposure can be greatly reduced if computers connected to the campus network are regularly scanned for known security exposures.

**Monitoring Networks, Operating and Enterprise Systems, and Routers**

Most institutions surveyed (55 to 68 percent) monitor their networks, operating systems, and enterprise systems daily. Larger institutions and doctoral institutions are more likely to monitor on a daily basis. According to the University of Washington’s Terry Gray, proactive vulnerability probing is one of the most important tools available to secure a population of computers. It is not a one-time activity but requires an ongoing and recurring effort. Regularly monitoring institutional networks for abnormal activity helps institutions identify incoming attacks, locate and isolate machines with known vulnerabilities, or react to security breaches in process.

**Incident-Response Procedures**

Respondents were asked if they had a formal IT security incident-response procedure. Forty-five percent did, with public and doctoral institutions and those with more than 25,000 students enrolled most likely to have these procedures in place. As enrollments increase, so does the likelihood that an institution will have a formal incident-response policy. Those institutions with formal incident-response procedures can respond to an incident quickly, ensure that damage is assessed, and effectively manage internal and external public relations. William Paraska, director of university computing and communications at Georgia State University, emphasized, “You have got to have a plan—you have to know what’s out there, what’s going to happen to you, and how you’re going to deal with it. Some schools are out there floundering—without an overall approach [to IT security].”

**Incidents**

Only 19 percent of our survey respondents reported that they had had an IT security incident that had been reported to the press. Larger institutions and doctoral institutions were more likely than other institutions to have had an incident reported in the press. Of the 19 institutions with enrollments of more than 25,000, 58 percent had an incident reported in the press. As the number of devices and users increases, the percentage of institutions with security incidents reported in the press increases dramatically.

**Impact of Residence Halls**

Residence halls connected to the campus network are often cited as a potential risk area. Of the institutions surveyed, 76 percent had residence halls. These institutions were more likely to have policies in place to shut off Internet access (89 percent versus 68 percent) and formal incident handling procedures (48 percent versus 34 percent) than institutions without residence halls connected to the network. It appears that the added risk posed by residence halls raised IT security awareness in general, resulting in the adoption of good practices.

**Successful Security Programs**

Respondents were asked several questions related to the perceived success of their IT security program. Overall, the respondents felt more secure today than they did two years ago but also felt that their IT security programs needed strengthening. Institutions, by and large, have not developed metrics for measuring their IT security programs’ effectiveness. The individuals we interviewed had varying opinions about
what constituted success. Bruce Judd, associate vice president for university computing and telecommunications at San Jose State University, stated, “Success is measured by the number of problems we have.” Dick Jacobson, IT security officer at the North Dakota State University System, reflected, “I think our program is effective, and the effectiveness has grown because of the formalized structure that we have put in place with the designated security officers on the campuses.” Morrow Long, director for information security at Yale University, noted, “IT [security] is effective: over time we have been able to achieve quite a bit in terms of increasing security…. It is an incremental, evolutionary approach, year by year—but we have moved quite a bit in terms of where we’ve come.”

Survey respondents who have IT security policies in place, dedicated IT staff, or security as part of their IT plan characterize their IT security program as successful and feel more secure today than they did two years ago. Also, at institutions where the president and provost are involved in policy development, the IT security program is viewed as more successful than at institutions where they are uninvolved. When IT security policies exist, the survey respondents reported feeling that the IT security program was successful.

**IT Security Barriers**

Our respondents indicated that the absence of resources was by far the largest barrier (72 percent) to IT security. When comparing the IT security budget share against the evaluation of IT security program success we found that institutions that spent the largest percentage of their total IT budget on security were more likely to view their security program as successful. Yet a dichotomy exists between the perceived importance of IT security (75 percent considered IT security as one of the top three institutional priorities) and the resources being made available (only 28 percent of institutions agreed or strongly agreed that their institutions were providing the necessary resources). Notre Dame’s CIO Gordon Wishon stated, “Justifying investment in security is very difficult because it is a negative deliverable. You only know when you don’t have security.” San Jose State University’s Bruce Judd noted how he obtained funding at his institution: “Because I have kept the president’s cabinet as well as the academic senate budget committee apprised with quarterly reports on network security and security issues, now they recognize the importance of network security. They raised security funding up to the mission-critical [level], whereas before it was viewed as just an option.” Other barriers to IT security that respondents identified included awareness (46 percent) and cultural reasons, such as academic freedom (32 percent) and culture of decentralization (30 percent).

**IT Security and Internal Business Practices**

One challenge of having security policies and practices is determining when and how to grant exceptions to the stated policy. A majority (55 percent) of our survey respondents indicated that business requirements take precedence over IT security when the two conflict. Only 17 percent of the respondents disagreed or strongly disagreed with this approach. This confirms the anecdotal belief that functionality takes precedence over IT security when new systems are installed. Some institutions, however, have found an acceptable balance by weaving their IT security into their business practices. According to Yale University’s Morrow Long, “In 1997 we built IT security into the new administrative system and into training…. HIPAA forced the medical school to increase information security awareness as well.”
IT Security: Not Just About Technology

Although using technology is necessary to achieve effective security, the human side often needs the greater attention. Fifty-two percent of the institutions in our survey agree or strongly agree that IT security problems inadvertently caused by authorized users are a significant concern. Despite this perception, nearly 66 percent of institutions reported having no formal awareness programs in place for students, faculty, or staff. Recommendations from higher education staff emphasize the importance of paying attention to user training and awareness. Notre Dame’s Gordon Wishon recommended, “Commit resources not only to technology solutions, but to education and awareness—particularly education and awareness among students and faculty, and certainly staff too.”

Andrew Conley, network security officer at South Dakota State University, advised, “You can put all the technology in place, but if you don’t let the users know, a lot of times they can find ways around it or they may do ‘bad’ things unknowingly. User awareness is one of the areas that really needs to be addressed in the security realm.” Larry Lidz, senior network security officer at the University of Chicago, recommended, “There are two main things—convince everyone that security is something they should be concerned about, and build up trust [among the user community].”

Conclusion

This ECAR study of IT security in higher education portrays an industry that is struggling to secure a culturally open environment against the rising tide of threats posed both from within and without higher education. In the main, survey respondents consider their institutions’ information resources to be secure, but most insist on the need for more resources to remain “in the fight.” The data strongly suggest that some investments and strategies work; investments in security experts and in a security organization are strongly associated with expressed feelings of security. On the other hand, lack of investment in efforts on the soft side of security, such as education and awareness programming, is highly associated with a reported sense of insecurity. It is clear that investments in the technologies of IT security are necessary. It is equally clear that these investments are insufficient.

IT security, in the end, comes down to people’s behavior. Most of the dramatic IT security risks relate to attacks by viruses, worms, super-worms, and the like. Perhaps the greatest damage is reflected in the opportunity costs of shutdowns in the wake of denial-of-service attacks, and the most bone-chilling risk may be that of identity theft. Even so, most hazards facing higher education fall into the gray area of unintended mistakes made by colleagues within our institutional bounds.

Endnotes

Introduction

We must strive for a sensitive balance between openness and security, between access and control. We need both.
—James Wright, President, Dartmouth College

P

roviding secure information technology (IT) services to colleges and universities is a special, if not unique, challenge. Unfettered and timely access for all to enormous quantities of information is higher education’s lifeblood and is key to its success in educating its students and generating new ideas and know-how. Insensitive, political, or casual attempts to check and control this dynamic transmission and consumption of information are problematic at best, and potentially deleterious to the academic mission. On the other hand, thoughtful and mission-minded implementation of IT security can and will ensure, protect, and facilitate the requisite flow of information so necessary for higher education’s continued success.

James Wright, president of Dartmouth College, captures higher education’s dilemma and posits on its future. “The new environment of higher education will require increased security, and new procedures may mandate changes in practices that have been used for many years.”¹ Indeed, much has changed since the early and mid-1990s when information security was more a local problem for selected institutional business and research units and the IT organization. With the advent of the World Wide Web in 1993 and the commercialization and globalization of the Web in the mid-1990s, the campus community’s attention to information security began to change, both rapidly and radically. Risks and threats to institutional information assets grew suddenly and exponentially as educational institutions were subjected to both accidental and malicious acts that exploited inherent network, operating system, and software vulnerabilities and low levels of security awareness and security-conscious behavior.² Noteworthy, too, was the change in federal and state legal environments, which mandate ever-stronger IT security practices. And public expectations of IT security for higher education—and all industries for that matter—are growing as well.

More than ever, higher education’s information assets, whether they support core missions or business administration, are essential to enhancing reputation, competitiveness, client satisfaction, revenue, and accountability, so they must be protected. And despite occasional academic and cultural resistance (or apathy), most institutions are investing substantial financial and human resources to protect their information infrastructure and valuable intellectual assets and, not least, the privacy and interests of the people they serve.

Indeed, we can compare IT security to fiduciary responsibility on the part of higher
education institutions. Just as institutions are held to standards regarding the accounting of their funds, so they are and will be increasingly held to standards of data protection. It is not surprising that auditors, both internal and external, are addressing these matters on a regular basis. How institutions will achieve acceptable levels of IT security, and by what means—technologies, policies, software, personnel, budgets—currently varies widely, as this study will demonstrate. But whether security is achieved and satisfactorily reported becomes less and less of an alternative. Indeed, higher education now faces the reality of providing robust IT security.

In a recent article in the *Chronicle of Higher Education*, Dan Carnevale elaborates on the implications of the Gramm-Leach-Bliley Act of 1999 for higher education. First thought applicable to financial institutions only, the legislation was largely ignored by higher education until the Federal Trade Commission ruled in 2002 that it also applied to colleges' and universities’ financial relationships. Higher education institutions therefore must notify people they deal with of their right to keep their financial information confidential and must protect their financial data. Protection also involves having a plan or security policy that includes designating an employee to coordinate information security, identify and repair computer system weaknesses, continually monitor systems, provide security training for employees, and ensure that service providers comply with the law through contract language requiring compliance.

As this study shows, institutions have proposed and implemented numerous IT security technologies and strategies. In many cases the investments haven’t proven sufficiently effective, however, especially as threats to institutions’ systems become commonplace and public scrutiny and press coverage become harsh and often unforgiving. Awareness training and other interventions that address behavior and institutional values also haven’t had the anticipated positive impact on internal security, largely because too few institutions have put them in place and many that have fail to deploy them regularly. Even where IT security measures are robust, failures abound.

The task appears daunting. Perhaps what most frustrates higher education’s senior administrators is coming to grips with the reality that IT security is an ongoing process of continual refinement and investment. They can never know whether the institution is really secure despite their best efforts, and there is no end point.

### What Do We Mean by Information Security?

By far the most commonly used meaning for information security in the literature is the preservation of:

- **confidentiality**, or protection from unauthorized use or disclosure of information;
- **integrity**, ensuring data accuracy and completeness through protection from unauthorized, unanticipated, or unintentional modification, and including **authenticity** (the ability of a third party to verify that a message’s content has not been modified in transit), **nonreputation** (the origin or receipt of a specific message must be verifiable by a third party), and **accountability** (an action can be traced uniquely to an entity); and
- **availability**, making data available to authorized users on a timely basis and when needed.

We can, in turn, characterize each of these six protection categories—confidentiality, integrity, authenticity, nonreputation, accountability, and availability—by level of sensitivity: high (grave injury to an institution), medium (serious injury), and
low (minor injury).

(See the sidebar “ISO Standards” for information about ISO/IEC 17799:2000 standards.)

The above nuances are significant for higher education, where much information used for teaching and research requires the highest level of integrity and availability but a low level of confidentiality. For public institutions, this also holds true for much of their financial information. However, in areas protected by FERPA (Family Education Rights and Privacy Act), HIPAA (Health Insurance Portability and Accountability Act), and the Gramm-Leach-Bliley Act, and for sensitive research data, all six of the protection categories must be at the highest level. A compromise in any one area potentially puts the institution at significant risk.

College and university administrators thus face the dilemma of how to build information systems that can support the institution’s public and open missions and academia’s intellectual curiosity while protecting the privacy and intellectual property of the institution and its community. Higher education’s information systems must be both open and closed, depending on what kind of information is being viewed and its intended use. Flexibility is essential, and it must accommodate campus security needs and cultural values alike.

According to Gordon Wishon, CIO, associate vice president, and associate provost at Notre Dame University, finding the balance is the $64,000 question. “I don’t know if we can guarantee that we can strike a precise balance, partially because the requirements and threats are always changing and the legislative landscape and technology are changing. Whether we achieve this is something that I think we will always be questioning.” For Philip Long, CIO at Yale University, “the overall strategy is that we want a controlled, open network. It is not completely open by default; it is opened by request. That is the punch line to our strategy—finding ways to run networks and network segments that are opened by request.”

Diana Oblinger, executive director of higher education, Microsoft, and former ECAR senior fellow, eloquently addressed this dilemma. For higher education, “intellectual freedom provides for free and open scholarly inquiry, freedom of information, and creative expression, including the right to express ideas and receive information in the networked world. One possible interpretation of intellectual freedom is that individuals have the right to open and unfiltered access to the Internet.” She further noted that “the academic culture tends to favor experimentation, tolerance, and anonymity—all characteristics that make it more difficult to create a culture of computer and network security.” The challenge is to appropriately balance values, risk, and realistic safeguards.

The legal and regulatory environment also poses many challenges for higher education. According to Kenneth Salomon and colleagues, “Federal laws have failed to keep pace with technological innovations. The result has been an atmosphere of uncertainty, in which already scarce university resources are increasingly strained by policy considerations and constrained by fears of legal exposure. The absence of a single set of standards further complicates the issue, leaving administrators and IT directors struggling to decide how best to protect their institutions, while at the same time not interfering with their educational mission. Navigating this maze is made even more difficult due to the fact that many of the laws are overlapping or apply differently to different institutional activities.”

HIPAA is a particular force at this time. In the 14th annual Healthcare Information and Management Systems Society (HIMSS) Leadership Survey (2003) of leaders in hos-
ISO Standards

ISO/IEC 17799:2000 uses an elaborate set of standards that includes

**System Access Control**
1) To control access to information
2) To prevent unauthorized access to information systems
3) To ensure the protection of networked services
4) To prevent unauthorized computer access
5) To detect unauthorized activities
6) To ensure information security when using mobile computing and telenetworking facilities

**System Development and Maintenance**
1) To ensure security is built into operational systems
2) To prevent loss, modification, or misuse of user data in application systems
3) To protect the confidentiality, authenticity, and integrity of information
4) To ensure IT projects and support activities are conducted in a secure manner
5) To maintain the security of application system software and data

**Compliance**
1) To avoid breaches of any criminal or civil law; statutory, regulatory, or contractual obligations; and of any security requirements
2) To ensure compliance of systems with organizational security policies and standards
3) To maximize the effectiveness of and to minimize interference to/from the system audit process

**Personnel Security**
To reduce risks of human error, theft, fraud, or misuse of facilities; to ensure that users are aware of information security threats and concerns and are equipped to support the corporate security policy in the course of their normal work; to minimize the damage from security incidents and malfunctions and learn from such incidents.

**Security Organization**
1) To manage information security within the institution
2) To maintain the security of organizational information processing facilities and information assets accessed by third parties
3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization

**Computer and Operations Management**
1) To ensure the correct and secure operation of information processing facilities
2) To minimize the risk of systems failures
3) To protect the integrity of software and information
4) To maintain the integrity and availability of information processing and communication
5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
6) To prevent damage to assets and interruptions to business activities
7) To prevent loss, modification, or misuse of information exchanged between organizations

**Asset Classification and Control**
To maintain appropriate protection of institutional assets and to ensure that information assets receive an appropriate level of protection. Included here are policies for asset classification, asset protection, asset management, acceptable use, vulnerability assessment and management, threat assessment and monitoring, and security awareness.

**Security Policy and Its Deployment**
To provide management direction and support for information security through document version control, difficulty of use—can you read and understand them?—distribution and ease of access, awareness, and compliance.
pitals, sponsored by the Superior Consultant Company, 61 percent of respondents—the second largest group in the survey—noted HIPAA compliance as having the biggest impact on them in the next two years (ranked second). Forty-three percent indicated that they would have to upgrade their IT systems’ security as a result.\(^7\)

Finding a correct balance proves extremely difficult in an open milieu with enormous network bandwidth, organizational diversity and autonomy, and a confusing legal environment, and where security breaches are increasing in number and notoriety. Moreover, for some insiders, compromising their institutional systems is a cottage industry—a personal challenge, perhaps just for fun.

**How Do We Establish Security Requirements?**

According to ISO/IEC 17799:2000, an international standard for information security management, there are three dimensions to establishing an institution’s security requirements. The first is through an institutional risk assessment, which is designed to determine the likelihood of internal and external threats to the institution and reveal its vulnerabilities. The second is the legal, statutory, regulatory, and contractual requirements imposed on the organization—for example, by HIPAA and FERPA. The third is the policies, procedures, and practices the institution has created for itself. This study does not focus directly on the legal environment but does try to determine whether higher education institutions have undertaken risk assessments and developed policies that help them establish security requirements.\(^8\)

**Security Threats and Breaches**

According to the ISO, a breach can be viewed conceptually as a vulnerability, a threat, or a risk. “A vulnerability is an error or a weakness in the design, implementation, or operation of a system. A threat is an adversary that is motivated to exploit a system’s vulnerability and is capable of doing so. Risk refers to the likelihood that a vulnerability will be exploited, or that a threat may become harmful.”\(^9\)

The combination of university systems’ open nature and the high-powered technology often present on campuses puts academic institutions in a unique position compared with other large enterprises. In addition to being the target of cyber attacks, university networks and systems sometimes serve either as the source of attacks on other entities or as a staging area for attacks on other entities by external hackers. This happened to Yahoo, Amazon, and eBay in February 2000. In this instance, a teenage hacker took control of computers owned by institutions including Stanford University, UCLA, and the University of California at Santa Barbara and used them to block access to these major e-commerce sites. For many institutions, being a good “net citizen” and preventing use of institutional resources for such attacks is nearly as high a priority as protecting their own information.

**Higher Education’s Responses**

Universities are responding to threats creatively by using new technologies and their substantial intellectual resources. At the University of Minnesota, Twin Cities, for example, the Minnesota Intrusion Detection System employs a suite of data-mining techniques to automatically detect novel and emerging attacks against computer networks and systems. The system has successfully detected attacks that are on the CERT (Computer Emergency Response Team) list of recent advisories and incident notes.\(^10\) Summarizing anomalous connections using association pattern analysis has been very
helpful in understanding the nature of cyber attacks and creating new signature rules for intrusion detection systems.

Increasingly, institutions provide education and professional training and are creating centers of academic excellence that undertake basic and applied research and development in information security. For example, in April 2003, Indiana University established the Center for Applied Cybersecurity Research to provide an environment where information security research and practice are intertwined, and Indiana University staff learn from each other. The center's goal is to maximize the speed with which new cyber research is applied and new cyber threats become the subject of research.¹¹

EDUCAUSE has long been recognized as a major participant in national efforts to secure higher education's communication and computing infrastructure. It has participated with Internet2 to conceive, develop, and deploy technologies, techniques, and standards to enhance identity services and other middleware elements essential to IT security. A joint EDUCAUSE/Internet2 Computer and Network Security Task Force has identified issues for further study, including how to make IT security a higher and more visible priority in higher education; using existing security tools more effectively; revising institutional policies; and designing, developing, and deploying improved security for future research and education networks. In the spirit of the Bush administration's national security goals, the task force seeks to raise the level of security collaboration among higher education, industry, and government and to integrate higher education work on security into the broader national effort to strengthen critical infrastructure.

The tragic events of September 11, 2001 made protecting the information infrastructure even more urgent. Securing cyberspace has become one of the pillars of the U.S. Department of Homeland Security's efforts. Especially noteworthy is the release of the Bush administration's cybersecurity plan on 14 February 2003. The national strategy addresses vulnerabilities of higher education institutions and acknowledges higher education's pledge to

- make IT security a priority;
- revise institutional security policy and improve the use of existing security tools;
- improve security for future research and education networks;
- improve collaboration between higher education, industry, and government; and
- integrate work in higher education with the national effort to strengthen critical infrastructure.¹²

In partial response to the federal initiative, EDUCAUSE, working with the American Council on Education (ACE) and the Higher Education IT Alliance, has recommended policies and measures necessary to realize greater system security. On 28 February 2003, ACE President David Ward urged university presidents to set the tone for information security on their campuses by insisting on community-wide awareness and accountability and establishing responsibility for campus-wide information security at the cabinet level. Further, presidents should routinely ask for a periodic information security risk assessment, manage risks in the context of institutional planning and budgeting, and regularly request updates to their institutions' information security plans to keep pace with the rapid evolution of the technologies, vulnerabilities, threats, and risks.

To contribute to the information infrastructure's national security, Indiana University partnered with the National
Infrastructure Protection Center (NIPC) in establishing the first higher education Information Sharing and Analysis Center in February 2003. The center’s goal is to help protect the nation’s colleges and universities from cyber attack and provide incident information to the NIPC.¹³

What’s Different About IT Security in Higher Education?

No study of IT security in higher education can ignore the common belief that higher education varies significantly from other industries and that IT security presents a different and extremely difficult challenge for IT security officers and administration. This view pervades the literature we reviewed. Diana Oblinger nicely captures many of the most common arguments.¹⁴ Briefly, many perceive higher education to be less secure in part because of its values such as academic freedom and freedom of expression, its decentralized organization, the mélange of hardware and software in use, and its unique mission and user base. As a consequence, the IT security strategies higher education must follow will differ and be more complicated than those in other industries. If higher education is different, do the dissimilarities, if real, make a difference?

Decentralization

In many collegiate environments, particularly larger ones, a decentralized culture is the norm. As a result, individual schools, laboratories, and departments may control a portion of any or all of the previously mentioned IT assets, making the job of the IT security administrator much more difficult. Rather than being able to automatically push new security patches out to all devices on the network or mandate the use of security tools like virus protection software, many university IT security officers find they must educate and persuade their user community to keep their machines secure.

In most corporate IT departments, centralization is the norm. The central IT organization controls hardware purchases, software loadsets (common sets of software installed on a computer), network infrastructure, user management, and most other aspects of computing within the organization. This enables corporations to centrally set security policies, make secure versions of operating systems and applications available to all users, control access to services being used on their network, and restrict or forbid use of insecure products and protocols.

Equipment Diversity

Even a small higher education institution’s technology environment varies significantly from the structure found in the corporate world. One of the biggest differences is that the institution does not actually own a large percentage of the machines on its network; many belong to students connected to the institution’s network in a dorm room or classroom. The technologies deployed at a typical college or university tend to be much more diverse than at a corporation. For example, a university network may have desktop machines from many vendors running multiple versions of Windows from 95 to XP, Macintosh PCs running several versions of the MacOS, and Linux workstations running several variants of that operating system. Software loadsets, if they exist at all, are likely created and managed at a departmental level. Server environments can be equally diverse, and many servers are purchased and administrated by semi-qualified staff or graduate students within schools, departments, or research labs.

For an IT security administrator, this diverse environment makes it difficult to
ensure that all systems are patched with the latest fixes or configured to limit security exposure. It also makes it difficult to provide IT security tools like antivirus software or personal firewalls to the university community because each platform needs a different version or even a completely different application. With so many machines not owned by the institution connected to the network, the security administrator must assume that there will always be insecure systems inside the perimeter and should expect to take additional steps to protect the institution that wouldn’t be necessary in the more controlled corporate environment.

In a typical corporate environment, technology standards control the type of equipment connected to the company’s network. Even in a large organization, all PCs and servers would be running the same operating system version, all similar hardware types would be purchased from the same vendor, and systems would use standard loadsets certified for security. Additionally, employees would be barred from putting rogue systems on the corporate network.

Mission Diversity
A typical university engages in many diverse business activities as part of its mission. In addition to teaching, many institutions conduct a wide range of research, provide hospitality services (dorms and dining halls), serve as ISPs and phone companies, engage in retail sales (bookstores, food concessions), manage financial accounts, and provide entertainment (athletics, arts), to name just a few. As a result, the IT environment of all but the smallest colleges is necessarily complex and constantly changing. And many institutions leave the selection and maintenance of systems used to support these functions to the individual business units.

For the security administrator, such complexity makes it more difficult to detect potential intrusions, because network traffic is much more unpredictable. Likewise, the diverse range of network services that must often be deployed, particularly at research institutions, makes it difficult to maintain effective firewalls. And the sheer number and diversity of applications the institution hosts makes it difficult for a central security organization to support each system, thus shifting the burden to the business units, which may not have the skills to maintain these systems.

Except at the largest corporations, IT security administrators in the private sector typically support an organization that conducts a limited range of business activities—for example, selling merchandise, managing financial accounts, or manufacturing products, along with the back-office functions that support this core activity. The IT environment needed to support these business activities is predictable, with relatively standard transaction flows and a limited set of network services required to enable these flows.

User Diversity
Corporate IT security administrators can generally assume that most legitimate connections coming from within their perimeter are being initiated by an employee of their organization. While such users can and do cause intentional security breaches, corporations can screen their employees for criminal backgrounds, mandate training, require the use of certain security technologies, and strongly enforce IT security policies.

However, for university security administrators, high-security-risk individuals are already inside the gates. On campuses with residential housing or wired classrooms, students freely connect insecure systems to the institution’s network and, not being employees, cannot easily be made to comply with training, policies, and other tools avail-
able to the corporate security administrator. In Chapter 7 we report that institutions with residence halls were nearly three times more likely to have experienced a significant security incident than those without.

In addition, universities are generally open environments. On many campuses, visitors can plug a laptop into any available data port and gain access to the institution’s network. Even in institutions that restrict such access, visitors can often use library machines, public kiosks, or machines in public computer labs, likewise giving them internal access to the network.

To mitigate the risks associated with non-employee network access, some institutions require all systems connected to the campus network to register their hardware address with central IT before they can use DHCP (dynamic host configuration protocol) servers to receive an IP address. This prevents random people from accessing the institution’s IP network using network ports in public spaces. Others require authentication to access any machine on campus, including lab and library systems. This is less of an issue for institutions that have chosen an IT security strategy that doesn’t rely heavily on perimeter firewalls, because having direct access to the network doesn’t provide a potential internal attacker significant advantage over an external attacker.

Research

Institutions that attract significant research funding have some unique issues of their own. By their nature, research labs encourage experimentation and often have extremely diverse computing environments, as explained by Michail Bletsas, director of computing at the Massachusetts Institute of Technology’s (MIT) Media Lab. “The central [IT organization at MIT] follows standards a lot closer than we do. We have no standards by design, because of the research nature of the facility. People are allowed to use whatever they feel like.” In addition, these systems may often store sensitive data, making them important to secure. However, partially because of the culture at many institutions and partially because of the rules governing coverage of institutional support costs from federal research grants, these systems are very often not under the purview of professional IT staff. Instead they reside in individual research facilities, managed on an ad hoc basis by graduate students.

Managing an IT security environment that incorporates a large research community therefore poses some special challenges for administrators. Several research universities we interviewed espouse an IT security philosophy seldom seen in the corporate environment: they make maintaining security on the institution’s desktop and server systems the responsibility of each system’s “owner.” To ensure that such an environment does not descend into chaos, these institutions’ central IT organizations provide their communities with common tools, such as antivirus software and operating system patch installers. They also conduct proactive monitoring of the systems connected to the institution’s network and alert system owners of any vulnerabilities or security breaches they discover, removing infected systems from the network if the problem is not or cannot be quickly corrected. It then becomes the system owner’s responsibility to remediate the problem before the system is allowed back on the network. Such an approach may not work for every institution, but those currently using it find it allows relatively small IT security teams to manage very large environments with few, if any, major incidents.

What Are We Protecting?

Most of the information stored on the systems of for-profit entities is confidential in
nature. From trade secrets to financial data to customer and employee information, such data is not made public, and corporations face serious financial consequences should such data be compromised. For example, the 2003 CSI/FBI Computer Crime and Security Survey reported that theft of proprietary information caused the highest losses for any type of IT security incident ($70.2 million, of approximately $202 million in total losses reported by 251 of their survey respondents). Denial-of-service attacks generated the second-highest losses ($65 million), as such attacks can quickly disrupt the core business of many enterprises. As a result of this large financial exposure, many for-profit entities strongly emphasize IT security, with the average respondent to Information Week’s 2002 Global Information Security Survey spending approximately 12.4 percent of their overall IT budget on security. The average salary for information security managers in industry, as reported by Information Security Magazine in August 2002, is $121,000 per year.

By contrast, in higher education much of the data institutions store is not considered sensitive. At many public institutions, financial data and employee salaries are considered public records, making the expenditure of significant time and effort to secure them less important. Some information, of course, such as donor records, research data, and personal information about students and employees, is private. For the most part, universities seem to focus more on providing a trusted technology environment to enable their constituents’ work rather than protecting data stored on their systems. John Curry, executive vice president at MIT, said, “I tend to think of security starting first and foremost with people, and their ability to live and work here. This leads in turn to the need for security personnel and technologies, from streetlights to fire protection to data protection. We want to provide [our community with] a sense that your computer is a safe thing to use. We want to protect their productivity.”

Additionally, denial-of-service attacks are less of an issue for most higher education institutions. While a disruption to network services in the middle of a registration cycle, for example, would be a major annoyance, it would not curtail the university’s ability to teach courses, conduct research, or otherwise carry out much of its day-to-day business (although this could change if distance learning becomes a larger part of the curriculum).

We feel that this disparity in exposure may be at least partially responsible for much of higher education’s perceived underinvestment in IT security, because the financial risks institutions face amount to significantly less than those faced by comparably sized for-profit businesses. For example, results presented in Chapter 5 show that 78 percent of our survey respondents spend 5 percent or less of their central IT budget on security and that only 11 percent of respondents pay their IT security managers more than $100,000. This may not be an underinvestment at all but rather a decision by senior executives that IT security, as part of the overall portfolio of risks the institution faces, may not warrant as high a level of investment as it does in other industries. However, recent legislation, such as HIPAA and Gramm-Leach-Bliley, that includes IT and data security provisions may change this calculation, as these regulations include significant penalties for noncompliance.

**Need for More Study: ECAR’s Role**

Despite the national attention and ongoing efforts of EDUCAUSE, Internet2, and other organizations to develop and foster a modern and secure IT infrastructure in higher education, our knowledge
of the current state and future plans of colleges and universities vis-à-vis IT security is largely anecdotal. We have little quantitative information with which to benchmark IT security. Security leadership is purported to be reactive rather than proactive, with a lack of clearly defined goals. Similarly, the academic culture is purported to believe that security is antithetical to academic and intellectual freedom.

This ECAR study is designed to provide a first empirical perspective of higher education’s security environment, one that we anticipate will lead to information security improvements across the sector. It establishes a security baseline for higher education. It identifies what security policies, products, and procedures are currently in place. College and university administrators will be able to compare their institution’s investments and practices with those of similar institutions. This is a necessary first step in determining the security level that needs to be sought. Systematic quantitative data also makes it possible to assess what heretofore has been anecdotal information about IT security in higher education as well as some myths that surround IT security.

This report emphasizes both the benefits and risks of implementing security solutions while considering trade-offs and future trends. We expect this data to contribute to the improvement of information security for higher education. If demonstrating information security to the public becomes as important as demonstrating institutional fiduciary responsibility, then benchmarking what is currently in place will be a critical step toward establishing standards for demonstrating IT security.

One message will become clear as we present the data in this study: higher education is all over the map when it comes to IT security. At the same time, we can discern several trends that suggest increasing agreement on standards, organization, and practices. The question is, How soon do we reach an agreement?

Endnotes
2. The CERT Coordination Center (CERT/CC) reported that IT security incidents grew from 252 in 1990 to 82,094 in 2002. In 1995, 171 vulnerabilities were reported compared to 4,129 in 2002. See <http://www.cert.org/stats/#incidents>.
4. NIST Special Publication 800–26, Security Self-Assessment Guide for Information Systems, Nov. 2001, pp. 5–6. The U.S. National Institute of Standards and Technology provides an alternative definition for information infrastructure protection. By information infrastructure they mean “technologies, processes, and activities to protect information infrastructures from hostile threats, to detect unauthorized or potentially damaging behavior, to react to detected or suspected incidents, and to ensure accountability for actions involving information infrastructure components. Legal, policy, and cultural imperatives that constrain or otherwise influence the way technology is used or developed are integral to the concept of an information infrastructure.”
6. K. D. Salomon, P. C. Cassat, and B. E. Thibeau, Electronic Information Security: A Legal Perspective (Dow, Lohnes & Albertson, PLLC, Feb. 2003). The EDUCAUSE/Internet2 Computer Network Security Task Force commissioned the work, and the authors received a grant from the National Science Foundation. Their work provides an overview of the current legal landscape and factors that foster an atmosphere of confusion and uncertainty as to how to proceed in the current legal environment. The paper summarizes existing federal and state privacy and security-related laws affecting institutions of higher education and explains their implications.
7. HIMSS (Healthcare Information and Management Systems Society) is the healthcare industry’s only membership organization exclusively focused on providing leadership for the optimal use of health-
care information technology and management systems for the betterment of human health. HIMSS is the equivalent of EDUCAUSE for the healthcare provider industry.


9. Ibid.

10. The CERT Coordination Center (CERT/CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.


The ECAR IT security study used a multi-faceted research methodology to gather both quantitative and qualitative data from 435 higher education institutions (414 U.S. institutions and 21 Canadian). We believe this is the single most comprehensive gathering ever of IT security information in higher education. The data provide a view of one segment of higher education’s collective experience with IT security as well as in-depth institution-specific perspectives. Note that some tables presented in this study will have fewer than 435 respondents; we adjusted these tables for missing information.

Research Approach

We undertook five data collection and analytical initiatives: a literature review, consultation with a select group of IT security leaders in higher education, a quantitative Web-based survey, qualitative telephone interviews, and four in-depth case studies.

The literature review helped identify and clarify issues and create a working set of hypotheses to be tested. However, the extant work focusing primarily on higher education and IT security is minimal. The vast majority of the electronic magazine literature focuses on business. Books and articles in professional journals analyze available technologies. Exceptions are the publications of EDUCAUSE and the Chronicle of Higher Education. The federal government’s publications and the professional organizations place great emphasis on planning, policies, preparedness, and awareness.

We paid particular attention to IT security surveys undertaken by the various security magazines, often with the assistance of consulting firms. When appropriate, we included questions that mirrored those in these surveys, which enables a limited but useful comparison of higher education with other sectors of the economy.

Because security technologies and practices are undergoing such rapid change, probably the best information available is on the Web. We include a short bibliography (Appendix D) listing the Web sites we used and found helpful. This bibliography is not intended to be comprehensive.

Consulting with IT security leaders in higher education helped us identify and validate the most interesting research questions and hypotheses that would frame the construction of a quantitative survey instrument. Richard Katz’s foreword to this study acknowledges their participation. On the basis of these discussions and the literature review, a research framework was finalized in February 2003, allowing development of the online survey to begin.
ECAR fellows and staff and John Vouloudakis of Cap Gemini Ernst & Young designed a quantitative Web-based survey. EDUCAUSE staff sent an e-mail invitation with the survey's Web address and access code information to 1,473 EDUCAUSE member institutions. Senior college and university administrators, most of them CIOs and other IT leaders, from 435 institutions responded to the survey. Their responses provide a detailed understanding of how higher education approaches IT security. The survey questions appear on the ECAR Web site, <http://survey.educause.edu/survey/it-security_preview.html>. Appendix B lists institutions that responded to the survey. We note that the information collected is confidential. We present no quantitative survey data that would make it possible to identify a particular institution or respondent, and the data files used for analysis were purged of any data that would have similar consequences.

Qualitative telephone interviews with 42 information technology executives, managers, and faculty members at 18 institutions provided in-depth information on key IT security issues (see Appendix A for names of participating individuals). We selected interviewees on the basis of peer nomination. In addition, we chose institutions that had responded to the core survey as follows:

- They characterized their IT security program as highly successful.
- They agreed or strongly agreed that their institution had gone beyond federal and state government recommendations for IT security.
- They agreed or strongly agreed that their institution had provided needed resources to address IT security issues.
- They had had a significant incident reported in the press.
- They had formal institutional IT security policies in place at their institution.
- They had at least one full-time central IT security staff member.

The institutions chosen were:
- Austin Community College
- Embry-Riddle Aeronautical University
- Emory University
- Florida Memorial College
- Georgia State University
- Humboldt State University
- Maricopa Community Colleges
- North Dakota University System
- Pace University
- Portland State University
- South Dakota State University
- University of California, Irvine
- University of Chicago
- University of Michigan–Ann Arbor
- University of Notre Dame
- University of Wisconsin–Madison
- Westminster College
- Yale University

All subject institutions are EDUCAUSE members. To obtain adequate depth and breadth of practice, we chose institutions that varied in size and mission, and included both public and private institutions.

We conducted four in-depth case studies. The first three focused on single institutions: the Massachusetts Institute of Technology, Indiana University, and the University of Washington. All three have deployed exemplary security systems from which others may learn effective practices. The fourth case study examines management procedures for press-reported security incidents at the Georgia Institute of Technology, the University of Montana, and The University of Texas at Austin. These case studies are designed to complement the core study and will be published separately.
We did not include the following topics in this study because they are important and large enough to warrant separate study:

- business continuity or disaster recovery,
- physical security,
- legal and ethical issues (such as copyright violations, pornography),
- legislative mandates (for example, FERPA, HIPAA, TEACH Act),
- specific technologies by vendor,
- software licensing,
- confidentiality, and
- privacy.

Carnegie Class As a Distinguishing Factor

The study grouped the sample by a modified Carnegie Classification of Institutions of Higher Education. The Carnegie taxonomy describes the institutional diversity in U.S. higher education. Most higher education projects rely on the classification to ensure a representative selection of participating individuals and institutions. We also believe that security strategies will differ by Carnegie class because missions, academic culture, and size vary significantly for each Carnegie group.

The study collapsed the categories as follows to obtain larger numbers for statistical and descriptive purposes:

- Doctoral/research universities—extensive (Dr. Ext.) typically offer a wide range of baccalaureate programs and graduate education through the doctorate. They award 50 or more doctoral degrees per year in at least 15 disciplines.
- Doctoral/research universities—intensive (Dr. Int.) typically offer a wide range of baccalaureate programs and graduate education through the doctorate. They award at least 10 doctoral degrees per year in three or more disciplines, or at least 20 doctoral degrees per year overall.
- Master’s colleges and universities (MA) typically offer a wide range of baccalaureate programs and graduate education through the master’s degree. The study grouped both Master’s Colleges and Universities I and Master II together.
- Baccalaureate colleges (BA) are primarily undergraduate colleges with major emphasis on baccalaureate programs. The study grouped the three baccalaureate college groups into a single BA group.
- Associate’s colleges (AA) offer associate’s degrees and certificate programs but, with few exceptions, award no baccalaureate degrees.
- Specialized institutions (Specialized) offer degrees ranging from the bachelor’s to the doctorate and typically award most degrees in a single field. Specialized institutions include theological seminaries and other specialized faith-related institutions; medical schools; medical and other separate health professions; schools of engineering and technology; schools of business and management; schools of art, music, and design; schools of law; and teachers colleges. The data presented for these schools must be interpreted in light of the enormous diversity of institutions within this category. We also provide data, where appropriate, on higher education system offices and for the 21 Canadian institutions in our study, recognizing that they vary by size and mission. We elaborate on differences between public and private institutions. Forty-three percent of the institutions in our study are private; 57 percent are public. We found little difference, however, along this dimension.
Institutions Surveyed and Their Characteristics

Figure 3-1 compares the distribution of the institutions that responded by their new Carnegie class, EDUCAUSE membership, and the universe of higher education institutions in the United States. The responding schools much more closely mirror the EDUCAUSE membership than they do the national population of institutions by Carnegie class. We have strong participation from doctoral-extensive institutions (52 percent) and doctoral-intensive institutions (30 percent), but the survey is weaker in terms of the other Carnegie classifications. We found that for IT security, however, the number of devices on the network rather than Carnegie class often proved a more significant differentiator.

Note also that the study relied on volunteers to complete the survey rather than on a random sample, and this limits the statistical conclusions that are possible. Nevertheless, the overall 30 percent response rate from EDUCAUSE member institutions gives us confidence that the study’s respondents portray a reasonable image of the EDUCAUSE membership, especially for doctoral and master’s institutions.

A statistical analysis of the data’s representativeness proved inconclusive. The findings do not support the conclusion that the institutions surveyed represent the population as a whole. Nor do they support the opposite conclusion that the respondents fail to represent the EDUCAUSE membership. Neither conclusion is statistically significant.

Institution Size: Number of Students, Network Users, and Devices

IT security literature on the business sector uses size as a significant variable that explains, in part, how much corporations are willing to spend on security. The larger the corporation and the greater the number of users, the lower the per-capita expenditure on security. Does size make a difference in higher education? We tested several hypotheses that consider the impact...
of size on various aspects of IT security by looking at the number of enrolled students, the number of users on the network, and the number of devices on the network.

The mean student enrollment of the institutions in our study was 7,169. For purposes of analysis, we’ve divided the institutions into six groups, as shown in Figure 3-2.

Smaller institutions dominate our study. Forty-nine percent have 4,000 or fewer enrolled students. Only 5 percent of the institutions in the study have more than 25,000 students. But that is the reality of the higher education environment.

**Connected Devices, Users**

Figure 3-3 shows the number of devices connected to institution networks. Sixty-one percent of the institutions in our study have 5,000 or fewer devices, and 79 percent have 10,000 or fewer. Less than 5 percent have more than 40,000 devices on their networks.
Much the same can be said for number of users, as Figure 3-4 shows. Sixty-one percent of the institutions have 10,000 or fewer users, and 74 percent have 20,000 or fewer. Less than 12 percent have more than 40,000 users on their networks.

Institutions with more than 10,000 devices and 20,000 users are for the most part public and, not surprisingly, doctoral institutions. We found that respondents for institutions having the most users on a network also had the most professional security experience.

**The Respondents: Position and Experience**

The survey was completed largely by CIOs (42 percent), chief IT security officers (12 percent), and other IT staff (38 percent) and reflects their experiences, observations, and opinions on IT security (see Figure 3-5). Academic, financial, and other administrative officers represent 8 percent of the respondents. We emphasize that this study largely represents a CIO/IT management view of IT security moderated by other institutional leaders’ observations obtained through complementary in-depth qualitative surveys and by those of the study’s advisors.

Of the 180 CIOs who answered the survey, 80 percent work at master’s, baccalaureate, and associate’s institutions. In contrast, 63 percent of the 53 chief information security officers who completed the survey held their positions at doctoral institutions. For the doctoral-extensive institutions only, the chief information security officer was more likely than any other position to complete the survey. At all other Carnegie class institutions, the CIO most often completed the survey.

The respondents, as a whole, have extensive IT security experience (see Figure 3-6). Forty-six percent of respondents indicated...
that they had more than 10 years of IT security experience, and more than two-thirds had at least six years of experience. Less than 10 percent had two years or less IT security experience. We found no difference in these percentages between private and public institutions. To a very small degree, associate's institutions had fewer individuals with 10 years or more experience, but the small sample size leads us to caution against generalizing from our data.

Years of IT security experience viewed by administrative position is worth noting. Sixty-one percent of the CIOs had 10 years or more of IT security experience (67 percent in Canada), and 79 percent had six years or more of experience (77 percent in Canada). Directors of administrative computing had
the most IT security experience, with 62 percent having 10 years or more and 85 percent having six years or more. Ironically, the position with the least experience was that of IT chief security officer. Thirty percent of IT security officers completing the survey had 10 years or more of experience, and 51 percent had six years or more.

Our respondents bring a great deal of experience to our study and provide a broad view of IT security from a variety of IT positions and institutions within higher education. We are gratified by the number of respondents, which makes the findings more than simply the observations of a small subset of the industry. In the chapters that follow, we present respondents’ collective view of IT security in higher education. Chapter 4 provides an overview of the security technologies in use at 435 institutions. In Chapter 5 we describe the security culture—the human side of IT security, by which we mean leadership and organization, values, and rules embodied in policies and procedures.

Endnotes
2. The Carnegie Classification of Institutions of Higher Education recognizes 1,669 associate's institutions, whereas the American Association of Community Colleges (AACC) membership currently includes 1,171. The AACC numbers are based on the definition of colleges eligible for membership in the AACC constitution: colleges that award the associate degree and are regionally accredited. The Carnegie count includes career colleges and colleges accredited by the Accrediting Council for Independent Colleges and Schools.
This chapter explores the information security technologies used by the institutions in our survey. What tools have they chosen to install to prevent harm to their information assets? Do we find differences among the institutions? For example, do institutions with many devices on their networks pursue different IT security strategies than those with fewer devices? Are there differences among Carnegie class institutions? And how does higher education compare with industry? Is it true that higher education lags the private and corporate sectors in installing security technologies?

We define the technologies discussed here by functionality, locus or scope of use, objectives, and the threats they address.¹

Security Technologies in Use

The data we collected portray a fairly comprehensive view of security approaches that our subset of higher education institutions currently have in place, are implementing, or are piloting to prevent cyber attacks. We asked institutions in the planning stage when they expect to undertake various security approaches. We also determined if an approach was even under consideration.

Table 4-1 presents the data in rank order of use. Secure Sockets Layer (SSL), centralized data backup, and perimeter firewalls are most in use or under way, followed by interior firewalls, enterprise directories, virtual private networks (VPNs), and intrusion detection. For most institutions, electronic signatures are either not under consideration or at best are 12 to 24 months out. While the data for Shibboleth² are similar, its adoption rate is increasing since we completed the survey.

Not surprisingly, we find a great emphasis on firewalls combined with antivirus software as a solution to network security. This combination is used by 97 percent of the ECAR survey institutions. Fully 87 percent of the institutions responding to the survey have installed either an interior or perimeter firewall or both. Another 10 percent are currently installing firewalls, which will bring these higher education institutions to the level other survey data show for industry. Of the institutions that have implemented interior firewalls, 80 percent have also installed...
Of the institutions that have installed perimeter firewalls, 56 percent have also installed interior firewalls. The 2002 EDUCAUSE Core Data Service survey corroborates these findings.

Firewalls, however, have their problems and trade-offs. According to Terry Gray, University of Washington, “firewalling,” or perimeter protection, “is about policy-based packet filtering at specific physical or logical points in a network—that is, blocking certain packets from proceeding to their intended destination. It is a defensive strategy implemented at the network transport layer of a system hierarchy. Sometimes the implementation is done on the host and sometimes it is part of the network infrastructure itself.” Gray further noted that “a growing num-

### Table 4-1. Status of Security Approaches Used

<table>
<thead>
<tr>
<th>Security Technology</th>
<th>Implemented</th>
<th>In Progress</th>
<th>Piloting</th>
<th>In 12 Months</th>
<th>In 24 Months</th>
<th>Not Being Considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL for Web transactions</td>
<td>73.2</td>
<td>12.9</td>
<td>3.1</td>
<td>5.0</td>
<td>3.1</td>
<td>2.6</td>
</tr>
<tr>
<td>Centralized data backup</td>
<td>71.0</td>
<td>10.7</td>
<td>2.8</td>
<td>4.2</td>
<td>5.4</td>
<td>5.8</td>
</tr>
<tr>
<td>Network firewall (perimeter)</td>
<td>70.9</td>
<td>11.0</td>
<td>2.6</td>
<td>4.4</td>
<td>3.3</td>
<td>7.9</td>
</tr>
<tr>
<td>Network firewall (interior)</td>
<td>50.0</td>
<td>18.6</td>
<td>3.8</td>
<td>9.4</td>
<td>8.3</td>
<td>9.9</td>
</tr>
<tr>
<td>Enterprise directory</td>
<td>48.2</td>
<td>24.1</td>
<td>4.9</td>
<td>9.1</td>
<td>7.6</td>
<td>6.1</td>
</tr>
<tr>
<td>VPN for remote access</td>
<td>45.4</td>
<td>17.8</td>
<td>8.8</td>
<td>12.4</td>
<td>8.1</td>
<td>7.6</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>42.8</td>
<td>15.1</td>
<td>10.4</td>
<td>13.7</td>
<td>15.6</td>
<td>2.4</td>
</tr>
<tr>
<td>Intrusion prevention tools</td>
<td>33.1</td>
<td>15.3</td>
<td>10.9</td>
<td>16.1</td>
<td>18.0</td>
<td>6.6</td>
</tr>
<tr>
<td>Encryption</td>
<td>31.8</td>
<td>19.5</td>
<td>9.9</td>
<td>9.9</td>
<td>16.6</td>
<td>12.3</td>
</tr>
<tr>
<td>Content monitoring/filtering</td>
<td>31.6</td>
<td>10.9</td>
<td>4.9</td>
<td>5.9</td>
<td>10.9</td>
<td>35.8</td>
</tr>
<tr>
<td>Standards for application and system</td>
<td>30.0</td>
<td>21.6</td>
<td>4.1</td>
<td>14.8</td>
<td>12.2</td>
<td>17.3</td>
</tr>
<tr>
<td>development</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic signature</td>
<td>6.5</td>
<td>7.8</td>
<td>8.5</td>
<td>10.3</td>
<td>30.5</td>
<td>36.5</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>1.1</td>
<td>3.5</td>
<td>4.9</td>
<td>7.1</td>
<td>24.7</td>
<td>58.7</td>
</tr>
</tbody>
</table>
ber of security professionals recognize that a network-centric approach to security is at best inadequate and at worst dangerous if it lessens focus on host security—especially in an environment where vast numbers of quasi-independent units with wildly differing computing needs share the same network infrastructure.”

On a further note of caution, Gary Dobbins, director of information security, University of Notre Dame, stated, “Selecting the technology or overall strategy is not the difficult aspect of the job. Integrating it with current or future practices is the lion’s share of the work there. For example, fitting a firewall into an existing data center without disrupting current services, and retraining and realigning processes and procedures around it can take a great deal of time and effort as well.”

**Interior Versus Perimeter Firewalls**

Baccalaureate institutions (83 percent) were twice as likely as doctoral institutions (40 percent) to have perimeter firewalls (see Table 4-2).

### Table 4-2. Security Approaches Adopted, by Carnegie Class and Canada

<table>
<thead>
<tr>
<th>Security Approach</th>
<th>Adoption, by Carnegie Class (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dr. Ext.</td>
</tr>
<tr>
<td>SSL for Web transactions</td>
<td>81.8</td>
</tr>
<tr>
<td>Centralized data backup</td>
<td>61.8</td>
</tr>
<tr>
<td>Network firewall (perimeter)</td>
<td>40.3</td>
</tr>
<tr>
<td>Network firewall (interior)</td>
<td>49.4</td>
</tr>
<tr>
<td>Enterprise directory</td>
<td>48.1</td>
</tr>
<tr>
<td>VPN for remote access</td>
<td>53.2</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>53.2</td>
</tr>
<tr>
<td>Intrusion prevention tools</td>
<td>34.2</td>
</tr>
<tr>
<td>Encryption</td>
<td>32.5</td>
</tr>
<tr>
<td>Content monitoring/filtering</td>
<td>19.5</td>
</tr>
<tr>
<td>Standards for application and system development</td>
<td>19.5</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>9.1</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>2.6</td>
</tr>
</tbody>
</table>
Perimeter firewalls were more often found at smaller enrollment institutions (see Table 4-3). For example, 80 percent of institutions with 4,000 or fewer students had perimeter firewalls versus 50 percent of institutions with 15,001 or more enrolled students. By contrast, interior firewalls were more often in place at larger institutions, where 74 percent of institutions with more than 25,000 enrolled students have interior firewalls versus approximately 48 percent for everyone else.

Sixty-eight percent of Canadian institutions had interior firewalls versus 48 percent of U.S. institutions. In general, a higher percentage of Canadian institutions employed security approaches—most employed more—than their U.S. counterparts. Canadian institutions, as a group, look more like the U.S. doctoral-extensive Carnegie class than they do smaller U.S. institutions.

Terry Gray described the large-school strategy: “Border firewalls have some long-term negative consequences, such as encouraging people to tunnel all manner of applications through ports that are rarely blocked by firewalls, and increasing the time it takes to troubleshoot problems with networked applications.” He suggested a strategy of “open networks, closed servers, and protected sessions,” by which he means pushing security perimeters and policy defini-

<table>
<thead>
<tr>
<th>Security Approach</th>
<th>Adoption, by Institution Size (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Up to 2,000</td>
</tr>
<tr>
<td>SSL for Web transactions</td>
<td>57.3</td>
</tr>
<tr>
<td>Centralized data backup</td>
<td>66.9</td>
</tr>
<tr>
<td>Network firewall (perimeter)</td>
<td>79.6</td>
</tr>
<tr>
<td>Network firewall (interior)</td>
<td>44.9</td>
</tr>
<tr>
<td>Enterprise directory</td>
<td>44.0</td>
</tr>
<tr>
<td>VPN for remote access</td>
<td>38.1</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>34.7</td>
</tr>
<tr>
<td>Intrusion prevention tools</td>
<td>32.5</td>
</tr>
<tr>
<td>Encryption</td>
<td>29.9</td>
</tr>
<tr>
<td>Content monitoring/filtering</td>
<td>31.6</td>
</tr>
<tr>
<td>Standards for application and system development</td>
<td>27.1</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>6.8</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>0.9</td>
</tr>
</tbody>
</table>
tion as close as possible to the organizations and computers to be protected, and making sure all sensitive traffic is encrypted. A one-size-fits-all strategy is problematic for the research university, and this approach serves the reality of the large institution. Tighter security is achieved by tailoring security to specific applications or needs of each small group or individual. Jeffrey Schiller, network manager at the Massachusetts Institute of Technology, agreed with this approach, saying, “Firewalls work best the closer they are to the assets they protect.”

Perimeter firewalls make sense at institutions where there are “homogeneous and simple computing requirements, the enterprise firewall is viewed solely as a defense-in-depth strategy, desktop configurations are tightly controlled by a central entity, and where performance and reliability concerns have been adequately addressed,” said Gray. He added that the research university fails this suitability test on all counts. However, the smaller institution, which quite often will not have the same level of IT resources as a large research institution, nor the same complex demands on its network, may well be served by a professionally managed perimeter firewall, which can reduce the amount of work needed to secure the rest of the institution’s network. Schiller warned, however, that “Firewalls can engender a false sense of security. A purchased firewall is not a substitute for professional [IT security] staff.”

Other Data Protection Strategies

The largest institutions were more likely to use enterprise directories, encryption, VPN, and electronic signatures, although we did find that 37 percent of institutions in every Carnegie class were not considering electronic signatures.

A VPN uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization’s network. It differs from an expensive system of owned or leased lines that only one organization can use. It works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, by encrypting data at the sending end and decrypting it at the receiving end, the protocols send the data through a “tunnel” that cannot be “entered” by data that is not properly encrypted. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses.

VPNs were in place at 63 percent of institutions with more than 25,000 enrolled students, compared with 40 percent for every other enrollment grouping. Fifty-seven percent of the Canadian institutions had installed VPNs versus 45 percent in the United States.

Shibboleth is developing architectures, policy structures, practical technologies, and an open-source implementation to support interinstitutional Web resource sharing subject to access controls. Using Shibboleth, the origin campus (home to the browser user) provides attribute assertions about that user to the target site. A trust fabric exists between campuses, allowing each site to identify another’s users and assign a trust level. Origin sites are responsible for authenticating their users but can use any reliable means to do this. Access-control decisions are made using the assertions. The origin site and the browser user control what information is released to the target.

Use of a centralized data backup system was lowest in doctoral-extensive institutions (62 percent versus 71 percent in general),
which is not surprising given the decentralized nature of computing at many institutions in this class. And this was one area where Canadian institutions lagged their U.S. counterparts (62 percent versus 71 percent).

Perhaps the most significant difference between large versus small institutions and doctoral versus other Carnegie class institutions concerned the use of SSL. This protocol uses encryption to secure communications between Web browsers and servers. Eighty-eight percent of institutions with more than 15,000 students had SSL; this dropped to a low of 57 percent at institutions with enrollments of 2,000 and under. Eighty-three percent of doctoral institutions had SSL versus 65 percent for everyone else, and 85 percent of Canadian institutions had SSL versus 73 percent in the United States. Intrusion detection and intrusion prevention tools follow a similar pattern. We are unsure whether this difference is due to expense or perceived complexity, or because smaller institutions are less likely to have Web-enabled applications that require secure connectivity.

Table 4-4 shows the rank order of strategies used by institutions in each Carnegie

<table>
<thead>
<tr>
<th>Security Approach</th>
<th>Rank, by Carnegie Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL for Web transactions</td>
<td>1</td>
</tr>
<tr>
<td>Centralized data backup</td>
<td>2</td>
</tr>
<tr>
<td>Network firewall (perimeter)</td>
<td>3</td>
</tr>
<tr>
<td>Network firewall (interior)</td>
<td>4</td>
</tr>
<tr>
<td>Enterprise directory</td>
<td>5</td>
</tr>
<tr>
<td>VPN for remote access</td>
<td>6</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>7</td>
</tr>
<tr>
<td>Intrusion prevention tools</td>
<td>8</td>
</tr>
<tr>
<td>Encryption</td>
<td>9</td>
</tr>
<tr>
<td>Content monitoring/filtering</td>
<td>10</td>
</tr>
<tr>
<td>Standards for application and system development</td>
<td>11</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>12</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>13</td>
</tr>
</tbody>
</table>
class and in Canada. It confirms perhaps more clearly the different approaches each subgroup is taking. The differences are small, with the major difference being the use of SSL and firewalls.

In summary, we found larger institutions (in terms of student enrollment) and Carnegie doctoral-extensive institutions more likely to have employed more of the available technology strategies, with a major difference in the use of perimeter firewalls. Institution size probably predicts what has been installed better than Carnegie class. A similar pattern occurs when we look at the number of users and devices on the network. For example, perimeter firewalls are used by 80 percent of institutions with 5,000 or fewer devices. But no institution in our survey with more than 100,000 devices used perimeter firewalls, and only 20 percent of the institutions with 80,001–100,000 devices employed them. Note, however, the small number of such institutions in our study. The number of devices differentiates institutions more strongly than number of users on the network.

Higher education rates somewhat lower in the use of these technologies than industry, as shown in Table 4-5. The table arrays survey findings from the ECAR survey; the 2003 CSI/FBI Computer Crime and Security Survey, sponsored by the Computer Security Institute; the 2003 Healthcare Information and Management Systems Society (HIMSS) Leadership Survey; and a 2002 KPMG survey. Note that these surveys’ methodologies, definitions, and sample sizes varied greatly, and the comparisons should be read with caution. Also, these surveys are snapshots in time of an environment that is rapidly and dynamically changing and where today’s preferred IT security technologies may quickly become obsolete. Adoption patterns may reflect this reality, especially where resources are limited.

The CSI/FBI survey found that 98 percent of their respondents had installed firewalls versus 87 percent in our study, and 73 per-

<table>
<thead>
<tr>
<th>Security Approach</th>
<th>Survey Population (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ECAR</td>
</tr>
<tr>
<td>Antivirus software</td>
<td>97</td>
</tr>
<tr>
<td>Network firewall</td>
<td>87</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>43</td>
</tr>
<tr>
<td>Encryption</td>
<td>32</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>7</td>
</tr>
</tbody>
</table>
The HIMSS survey indicated that 98 percent of the medical institutions used firewalls. More remarkable is that 56 percent used electronic signatures versus 7 percent for higher education, and 65 percent used data encryption versus 32 percent in our survey. However, a 2002 KPMG survey showed that only 14 percent of the respondents run a network-based intrusion detection system, and 15 percent run a host-based intrusion detection system.\(^5\)

What these data show is that the ECAR survey institutions are fairly comparable to industry in the use of firewalls and antivirus software. But our data also show that many ECAR survey institutions are in the process of implementing these technologies. This lag may be due to cost, but it may also be due to risk and the kind of data that need to be protected. The CSI/FBI survey noted that the greatest financial losses to businesses surveyed were from the theft of proprietary information ($70 million), denial of service ($65 million), and viruses ($27 million). Quite frankly, the first two risk areas do not have the same impact on higher education. Much of higher education’s information is public, and denial-of-service attacks, while inconvenient, would not devastate universities financially as they would an eBay or Amazon. It would cause dissatisfaction if registration, for example, were delayed a day or two, but teaching, research, and other core institutional functions could for the most part continue uninterrupted. Thus it may not make sense for higher education to invest as heavily as industry in some of these IT security technologies. The return on investment and perceived risk level may be too low to justify the investment. If this is true, the argument that higher education is under invested in security technologies may simply not be justified. The answer may be that higher education institutions face a different risk profile and therefore require a somewhat different set of solutions.

### Remote Network Access

Eighty-two percent of the institutions reported providing remote network access (see Figure 4-1). Public institutions (85 percent) are slightly more likely to provide remote access than private institutions (77 percent). Eighty-six percent of Canadian institutions provide remote access. All but two of the doctoral institutions provide remote access; two-thirds of the associate’s institutions provide remote access.

Seventy-six percent of the institutions (267 of 350 institutions responding to this part of the survey) provide a campus modem pool; 8 percent outsource; 26 percent arrange for a discount with an ISP; and 18 percent provide subsidized ISP accounts (Figure 4-2). We found only minor differences between public and private institutions.

Some institutions provide different services to faculty, staff, and students—for example, the campus modem pool may not be open to students, who would then purchase Internet service from a private ISP. In some instances, the campus pool is so limited that users go outside. And users will also go outside to get greater bandwidth. The University
Figure 4-1. Provision of Remote Access, by Carnegie Class

Figure 4-2. Network Access Provided by Institutions
of Minnesota, Twin Cities, for example, has negotiated a discount with an outside provider for students, faculty, and staff to obtain DSL or cable services at home.

We found some variation among the different Carnegie classes (see Figure 4-3). Doctoral-extensive institutions were most likely to have a campus modem pool (89 percent), and Canadian institutions were least likely (65 percent). Canadian and doctoral-intensive institutions were most likely to outsource, but the numbers are low. In addition, Canadian institutions were most likely to subsidize ISP accounts.

**Wireless Security**

Eighty-eight percent of institutions surveyed reported that wireless technology was installed on campus. The larger the institution’s enrollment, the more likely it had installed wireless technology. Seventy-eight percent of institutions with enrollments of less than 2,000 students reported that they provide wireless access, whereas 100...
percent of the institutions with enrollments over 15,000 did so. Carnegie class shows a similar pattern. All doctoral institutions, save one, report having wireless, compared with 78 percent of associate’s institutions. We noted a significant difference here with industry: the KPMG survey reported that only 10 percent of their participating firms have installed wireless networks.

Table 4-6 shows the status of technologies to secure wireless installations. Large institutions differ from smaller institutions, and doctoral institutions differ from master’s, baccalaureate, associate’s, and, to some degree, Canadian institutions in the use of strategies to secure wireless network access. Extensible authentication protocol (EAP), 128-bit wired equivalency privacy (WEP), and firewalls are more often used at master’s, baccalaureate, associate’s, and, to some extent, Canadian institutions. IP VPNs, Kerberos, and remote authentication dial-in user service (RADIUS) prevail at large-enrollment and doctoral institutions. Otherwise the usage pattern is similar for all institutions, with the seeming anomaly of 40-bit WEP being most heavily used at doctoral-intensive institutions (39 percent versus 20 percent for everyone else). We found little difference between public and private institutions.

We noted that fewer than half of the institutions have installed wireless encryption/authentication, and a majority of institutions

<table>
<thead>
<tr>
<th>Wireless Security Technology</th>
<th>Implemented</th>
<th>In Progress</th>
<th>Piloting</th>
<th>In 12 Months</th>
<th>In 24 Months</th>
<th>Not Being Considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>46.6</td>
<td>10.9</td>
<td>3.7</td>
<td>7.4</td>
<td>10.0</td>
<td>21.4</td>
</tr>
<tr>
<td>RADIUS</td>
<td>41.1</td>
<td>8.2</td>
<td>5.0</td>
<td>5.8</td>
<td>9.5</td>
<td>30.3</td>
</tr>
<tr>
<td>128-bit WEP</td>
<td>34.7</td>
<td>8.0</td>
<td>6.7</td>
<td>6.1</td>
<td>14.7</td>
<td>29.8</td>
</tr>
<tr>
<td>IP VPN</td>
<td>33.0</td>
<td>12.3</td>
<td>9.3</td>
<td>9.3</td>
<td>15.0</td>
<td>21.0</td>
</tr>
<tr>
<td>40-bit WEP</td>
<td>24.4</td>
<td>4.8</td>
<td>3.2</td>
<td>3.9</td>
<td>8.0</td>
<td>55.6</td>
</tr>
<tr>
<td>Vendor solution</td>
<td>18.5</td>
<td>4.0</td>
<td>4.3</td>
<td>3.1</td>
<td>8.9</td>
<td>61.2</td>
</tr>
<tr>
<td>Third-party hardware/software solution</td>
<td>17.6</td>
<td>5.6</td>
<td>6.3</td>
<td>4.7</td>
<td>10.7</td>
<td>55.2</td>
</tr>
<tr>
<td>EAP</td>
<td>14.8</td>
<td>7.2</td>
<td>7.2</td>
<td>9.3</td>
<td>21.7</td>
<td>39.7</td>
</tr>
<tr>
<td>Kerberos</td>
<td>12.2</td>
<td>4.1</td>
<td>6.3</td>
<td>4.4</td>
<td>16.6</td>
<td>56.6</td>
</tr>
<tr>
<td>AES</td>
<td>6.3</td>
<td>6.6</td>
<td>3.3</td>
<td>9.4</td>
<td>21.2</td>
<td>52.8</td>
</tr>
</tbody>
</table>
reported they are not considering implementing 40-bit WEP, vendor solutions, third-party hardware/software, Kerberos, or advanced encryption standard (AES). We also noted increased adoption of 128-bit WEP since the completion of the ECAR wireless survey in 2002. The data suggest that although clear standards have yet to emerge, institutions have deployed technologies to secure their wireless networks.

Rodney Peterson, EDUCAUSE security task force coordinator, found the above data to be disturbing. “It is remarkable that every approach is ‘not being considered’ by at least 20 percent or more of the institutions,” he said. “This suggests to me that we need to take a fresh look at wireless security—problems and solutions—and develop an appropriate strategy for educational institutions. The National Strategy to Secure Cyberspace spent a considerable amount of effort discussing the importance of wireless security for federal government agencies. The results of the survey suggest that a significant amount of work remains for higher education, possibly including shifting views about the threats of wireless networks to an institution’s overall security posture.”

One explanation for the level of insecurity emerged in our interviews: numerous respondents said they were not quite sure what to do about wireless security because of what they considered to be either inadequate or inappropriate standards. They seemed to be waiting to see how things would fall out.

**Authentication and Access Control**

Access control is a set of procedures and processes performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and limit access to a system’s resources to only authorized persons, programs, processes, or other systems. Authentication is a method for confirming a user’s identification, often as a prerequisite to allowing access to system resources.

At an August 2002 National Science Foundation workshop in Chicago organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force, a select group of higher education IT security officers and technology architects recommended priorities for an action agenda on security tools. Highest on the agenda for authentication was a proposal requiring that every network connection on campus, including those in the library, be accountable to a specific person via authentication or some other mechanism. Further, two-factor authentication—the use of multiple forms of authentication such as a combination of a PIN and a one-time-use password generated by a hardware token—should be established wherever necessary. Such authentication is generally used to protect critical systems or those containing confidential data.

We asked the respondents what methods they used for authentication. Table 4-7 shows what is currently used, in progress, or being piloted. We also asked what methods they were or were not considering and why. The respondents most frequently mentioned the criticality of the data needing protection and ease of use.

We found that traditional, multiple-use passwords predominate, and passwords and PINs in general are the accepted methods. Sixty-five percent of institutions reported having a policy on passwords. Passwords are problematic, however, as are many authentication tools. Andrew Conley, network security officer at South Dakota State University, noted that “fac-
Faculty or staff write down passwords and put them on monitors or under keyboards, especially with harder passwords because it is difficult to remember them. We need to train and educate them better about such practices.”

We found that 22 percent of respondents used Kerberos. Of the institutions using Kerberos, 49 percent are doctoral institutions, followed by MA institutions (11 percent). Thirty-seven percent of all doctoral institutions surveyed use Kerberos. Paul Howell, information systems security officer at the University of Michigan, noted that his institution has deployed Kerberos, and many campus systems leverage the Kerberos infrastructure. “However, we buy a lot of commercial software. Those products tend to know nothing about Kerberos. As a result, we have silo authentication schemes on campus.” Gregory Jackson, vice president and CIO at the University of Chicago, noted the “trade-off between the sophistication of a method and how broadly we can get it implemented. We’re going away from Kerberos (even though I think it’s a better method) to other forms of secure authentication such as SSH, SSL, or encrypted LDAP.”

More advanced tools such as PKI, tokens, smart cards, electronic signatures, and biometric technologies—user identification (and possibly access control) based on a physical, unchangeable characteristic such as a fingerprint, iris, face, voice, or handwriting—

<table>
<thead>
<tr>
<th>Authentication Technology</th>
<th>Implemented</th>
<th>In Progress</th>
<th>Piloting</th>
<th>In 12 Months</th>
<th>In 24 Months</th>
<th>Not Being Considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple-use passwords</td>
<td>72.9</td>
<td>7.3</td>
<td>0.5</td>
<td>1.2</td>
<td>5.1</td>
<td>13.0</td>
</tr>
<tr>
<td>Multilevel passwords</td>
<td>43.1</td>
<td>5.8</td>
<td>1.9</td>
<td>1.9</td>
<td>8.2</td>
<td>39.2</td>
</tr>
<tr>
<td>Password/PIN combination</td>
<td>40.2</td>
<td>5.6</td>
<td>1.3</td>
<td>3.8</td>
<td>15.9</td>
<td>33.3</td>
</tr>
<tr>
<td>Single-use passwords</td>
<td>39.2</td>
<td>6.1</td>
<td>2.8</td>
<td>3.0</td>
<td>11.1</td>
<td>37.3</td>
</tr>
<tr>
<td>Kerberos</td>
<td>22.0</td>
<td>4.2</td>
<td>3.9</td>
<td>3.9</td>
<td>14.1</td>
<td>51.8</td>
</tr>
<tr>
<td>PKI</td>
<td>9.8</td>
<td>5.8</td>
<td>8.2</td>
<td>5.6</td>
<td>28.6</td>
<td>41.9</td>
</tr>
<tr>
<td>Hard/soft tokens</td>
<td>8.1</td>
<td>2.2</td>
<td>3.3</td>
<td>3.1</td>
<td>17.2</td>
<td>66.1</td>
</tr>
<tr>
<td>Smart cards</td>
<td>7.0</td>
<td>3.6</td>
<td>5.2</td>
<td>2.3</td>
<td>27.6</td>
<td>54.2</td>
</tr>
<tr>
<td>Electronic signatures</td>
<td>6.7</td>
<td>5.2</td>
<td>9.3</td>
<td>8.0</td>
<td>32.0</td>
<td>38.9</td>
</tr>
<tr>
<td>Biometric technologies</td>
<td>1.1</td>
<td>0.5</td>
<td>4.0</td>
<td>0.3</td>
<td>18.2</td>
<td>75.9</td>
</tr>
</tbody>
</table>
ing—provide more reliable authentication but have low implementation rates. Most institutions are not considering tokens, smart cards, or biometric technologies.

Although institutions pursue different and multiple strategies, we did find that everyone uses something for authentication. As Figure 4-4 shows, 23 percent use only one form of authentication and 25 percent use two. But 42 percent use three or more forms of authentication, which stems in part from perceived levels of risk to particular information assets.

Choice of authentication methods is a policy decision at the University of Notre Dame. According to Gordon Wishon, CIO, associate vice president, and associate provost, the decision regarding when and where to use authentication is vetted with members of the university functional community. “We use an information security working group on campus with representatives from the student body, faculty, researchers, and IT support people across the campus and members of the functional community,” he explained. “In terms of selecting technology for authentication—that is a responsibility of the chief technology officer, working with the engineering group and the chief security officer.” For the most part, respondents to our in-depth interviews told us that authentication method choice depends on the perceived sensitivity of the data being protected.

Terry Gray considers static authentication credentials (ID and password) one of the greatest security risks. “One of the first steps in securing a network computing environment is to make sure that authentication credentials are always encrypted en route, either via secure application/access protocols (SSH, SSL, or Kerberos) or via transport-level encryption (such as VPNs).” Clearly, higher education has some way to go to reach Gray’s recommended security level. Failure to adopt these tools is especially unfortunate.

---

**Figure 4-4.** Number of Authentication Tools in Use
because recent Web browsers support SSL, and no additional client-side software or configuration of clients is required to implement this form of session/path protection.

Looking at what institutions are doing by Carnegie class and in Canada (see Table 4-8), we not surprisingly find that doctoral institutions apparently have taken the lead—small as it may be—in using new technologies. When viewing by number of devices on campus, we found little difference except in Kerberos use at the doctoral and larger enrollment institutions.

We asked respondents whether their institution had a unified login or single-sign-on system and found that 19 percent had implemented such a system and another 19 percent were currently implementing single sign-on. Forty-eight percent said they would implement such a system in the next two years; 14 percent said it was not under consideration. Doctoral institutions were more likely to have single sign-on in place. Of the institutions that had implemented a single-sign-on system, 43 percent had an enterprise directory.

Our findings closely track those of the 2002 KPMG study: the vast majority of their respondents (82 percent) still rely on user IDs and passwords. The survey’s researchers commented that the implementation of more robust forms of authentication has been slow and concluded that businesses have decided to accept the risk that tools such as biometrics could mitigate because of cost. The HIMSS respondents are much

### Table 4-8. Status of Authentication, by Carnegie Class

<table>
<thead>
<tr>
<th>Authentication Technology</th>
<th>Overall</th>
<th>Dr. Ext.</th>
<th>Dr. Int.</th>
<th>MA</th>
<th>BA</th>
<th>AA</th>
<th>Specialized</th>
<th>System</th>
<th>Canada</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple-use passwords</td>
<td>72.9</td>
<td>76.6</td>
<td>74.3</td>
<td>71.6</td>
<td>65.9</td>
<td>63.3</td>
<td>74.5</td>
<td>58.8</td>
<td>76.2</td>
</tr>
<tr>
<td>Multilevel passwords</td>
<td>43.1</td>
<td>39.2</td>
<td>40.0</td>
<td>32.7</td>
<td>42.0</td>
<td>37.5</td>
<td>50.0</td>
<td>35.3</td>
<td>47.6</td>
</tr>
<tr>
<td>Password/PIN combination</td>
<td>40.2</td>
<td>41.3</td>
<td>40.0</td>
<td>47.2</td>
<td>3.2</td>
<td>27.1</td>
<td>34.5</td>
<td>27.8</td>
<td>47.6</td>
</tr>
<tr>
<td>Single-use passwords</td>
<td>39.2</td>
<td>30.2</td>
<td>41.2</td>
<td>41.5</td>
<td>37.3</td>
<td>36.7</td>
<td>37.7</td>
<td>29.4</td>
<td>33.3</td>
</tr>
<tr>
<td>Kerberos</td>
<td>22.3</td>
<td>43.4</td>
<td>22.9</td>
<td>15.0</td>
<td>12.3</td>
<td>12.2</td>
<td>11.1</td>
<td>27.8</td>
<td>14.3</td>
</tr>
<tr>
<td>PKI</td>
<td>9.8</td>
<td>9.5</td>
<td>11.4</td>
<td>7.4</td>
<td>11.1</td>
<td>2.0</td>
<td>11.1</td>
<td>11.8</td>
<td>9.5</td>
</tr>
<tr>
<td>Hard/soft tokens</td>
<td>8.1</td>
<td>18.9</td>
<td>5.7</td>
<td>4.7</td>
<td>0.0</td>
<td>0.0</td>
<td>13.0</td>
<td>6.3</td>
<td>19.0</td>
</tr>
<tr>
<td>Smart cards</td>
<td>7.0</td>
<td>6.8</td>
<td>5.7</td>
<td>8.5</td>
<td>9.9</td>
<td>2.0</td>
<td>3.7</td>
<td>0.0</td>
<td>0.0</td>
</tr>
<tr>
<td>Electronic signatures</td>
<td>6.7</td>
<td>9.5</td>
<td>8.6</td>
<td>3.8</td>
<td>7.4</td>
<td>0.0</td>
<td>9.1</td>
<td>5.9</td>
<td>6.2</td>
</tr>
<tr>
<td>Biometric technologies</td>
<td>1.1</td>
<td>1.4</td>
<td>2.9</td>
<td>0.0</td>
<td>1.2</td>
<td>0.0</td>
<td>1.9</td>
<td>1.0</td>
<td>4.8</td>
</tr>
</tbody>
</table>
heavier users of multilevel passwords, most likely attributable to the sensitivity of patient data.

As Table 4-9 shows, the 2003 CSI/FBI Computer Crime and Security Survey reported that 11 percent of their respondents have installed biometric tools versus 1 percent in our study. HIMSS noted that 8 percent of the health organizations used biometric technologies but also indicated that 60 percent of their respondents planned to use biometrics in the next two years. HIMSS reported that 18 percent currently use PKI and 40 percent planned to use it in the next two years, compared with 10 percent and 36 percent in our study.

**Antivirus Protection**

Ninety-seven percent of institutions surveyed have installed antivirus protection on their operating systems, 90 percent on their application servers, 92 percent on their e-mail servers, and 88 percent on other servers. Georgia State University conducted an antivirus audit by sampling PCs across the university and found that they had 94 percent compliance. The overall figures compare favorably with the 99 percent finding of the 2003 CSI/FBI Computer Crime and Security Survey. Antivirus protection seems to go hand in hand with firewalls as a first line of defense, eliminating many worm and virus problems.

Sixty-eight percent of the institutions required that all institutionally owned systems have antivirus protection installed in order to be connected to the network, but only 36 percent required it of noninstitutionally owned systems. The requirement was weakest at large-enrollment and doctoral institutions. Baccalaureate institutions (87 percent) required it on institutionally owned operating systems, while only 30 percent of doctoral institutions required it. One factor that may explain the weaker requirements at large/doctoral institutions is the relative diversity of systems, some of which are not mainstream desktop systems with readily available antivirus solutions at competitive prices.

<table>
<thead>
<tr>
<th>Authentication Technology</th>
<th>Survey Population (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ECAR</td>
</tr>
<tr>
<td>Multiple-use passwords</td>
<td>73</td>
</tr>
<tr>
<td>Multilevel passwords</td>
<td>43</td>
</tr>
<tr>
<td>Password/PIN combination</td>
<td>40</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>19</td>
</tr>
<tr>
<td>PKI</td>
<td>10</td>
</tr>
<tr>
<td>Electronic signatures</td>
<td>7</td>
</tr>
<tr>
<td>Soft/hard tokens</td>
<td>8</td>
</tr>
<tr>
<td>Smart cards</td>
<td>7</td>
</tr>
<tr>
<td>Biometric technologies</td>
<td>1</td>
</tr>
</tbody>
</table>
Bruce Judd, associate vice president for university computing and telecommunications at San Jose State University, described his institution’s efforts in this area. “We have distributed or optional desktop support on campus historically. Some areas—hundreds of computers—have no desktop support, no updates or patching. That was one of the reasons we had so many problems [in the past]. A significant portion of our campus does not have any antivirus software running. We installed e-mail relays with antivirus at the gateway and then, because we have 40-plus e-mail servers, we had to start insisting that people begin putting antivirus on their servers. We have a licensing strategy that allowed us to buy software for our systems by platform and distribute it to compatible servers across campus. Those two strategies—e-mail relay with e-mail antivirus filtering plus site licensing antivirus software with a fixed number of user seats—have solved a lot of problems, especially with e-mail viruses and worms.”

Ninety-eight percent of the institutions had a site or volume license for antivirus software, but only 55 percent of the licenses covered personally owned computers. The larger the institution, the more likely it was to provide a license for personally owned computers. Ninety-four percent of institutions with more than 25,000 enrolled students provided such licenses versus 37 percent of institutions with 2,000 or fewer enrolled students. According to Gregory Jackson at the University of Chicago, “We hand out antivirus software like candy.”

In short, higher education is doing a good job installing and using antivirus software. But it appears that some institutions are reluctant to mandate usage, and some simply lack resources.

Strategies to Reduce IT Security Vulnerability

We asked institutions what strategies they were using to reduce IT security vulnerability, then rank ordered the strategies implemented. As Table 4-10 shows, strategies used most often include limiting protocols allowed through the firewall or router (76 percent), restricting or limiting access to

Table 4-10. Status of Strategies to Reduce IT Security Vulnerability

<table>
<thead>
<tr>
<th>Security Strategy</th>
<th>Implemented</th>
<th>In Progress</th>
<th>Piloting</th>
<th>In 12 Months</th>
<th>In 24 Months</th>
<th>Not Being Considered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit types of protocols through firewall</td>
<td>75.8</td>
<td>10.3</td>
<td>2.4</td>
<td>4.3</td>
<td>2.4</td>
<td>4.8</td>
</tr>
<tr>
<td>Limit access to servers/applications</td>
<td>72.4</td>
<td>11.6</td>
<td>2.1</td>
<td>4.5</td>
<td>3.5</td>
<td>5.9</td>
</tr>
<tr>
<td>Timeout access</td>
<td>68.0</td>
<td>9.9</td>
<td>2.7</td>
<td>3.4</td>
<td>3.7</td>
<td>12.3</td>
</tr>
<tr>
<td>Recovery plan in case of disaster</td>
<td>48.5</td>
<td>31.4</td>
<td>2.6</td>
<td>7.6</td>
<td>7.4</td>
<td>2.6</td>
</tr>
<tr>
<td>Install closed desktop system</td>
<td>36.2</td>
<td>14.0</td>
<td>6.5</td>
<td>3.9</td>
<td>8.2</td>
<td>31.2</td>
</tr>
<tr>
<td>Limit URLs through firewall</td>
<td>30.5</td>
<td>7.5</td>
<td>4.6</td>
<td>3.1</td>
<td>6.3</td>
<td>47.9</td>
</tr>
<tr>
<td>Install directory inventory system to detect change</td>
<td>13.0</td>
<td>11.2</td>
<td>6.9</td>
<td>7.9</td>
<td>20.9</td>
<td>40.2</td>
</tr>
<tr>
<td>Use security devices for authentication</td>
<td>12.3</td>
<td>3.5</td>
<td>4.9</td>
<td>3.4</td>
<td>21.4</td>
<td>54.5</td>
</tr>
</tbody>
</table>
servers and applications (72 percent), and timing out access to applications after an idle period (68 percent). Little used were installing a directory inventory system to watch for undesired program changes (13 percent) and security devices for personal authentication (12 percent). The latter two strategies and limiting URLs through firewalls were not under consideration at almost half of the institutions. We found, however, that limiting URLs through firewalls was a strategy more often implemented at BA and MA institutions (33 percent) than at doctoral-extensive institutions (17 percent). Perhaps what is most disturbing in these data is that only 48.5 percent report having a disaster recovery plan.

Table 4-11 shows the strategies being used by institutions in different Carnegie classes. Overall there is not much difference, but doctoral-intensive and baccalaureate institutions in general have implemented more strategies than the other classes have, and Canadian institutions have been more successful in limiting protocol types through firewalls (95 percent). The equipment installed also makes a difference. We noted earlier that 13 percent of the institutions had not installed firewalls. Therefore, we should see a proportionate use of limiting protocol types through firewalls.

With the exception of timing out access, the number of devices on the network does not seem to affect institutional strategies.

**Summary of Findings**

Higher education is adopting more technology to secure its information assets. But

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Implemented (Overall)</th>
<th>Dr. Ext.</th>
<th>Dr. Int.</th>
<th>MA</th>
<th>BA</th>
<th>AA</th>
<th>Specialized</th>
<th>System</th>
<th>Canada</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit types of protocols through firewall</td>
<td>75.8</td>
<td>59.2</td>
<td>82.9</td>
<td>73.1</td>
<td>81.2</td>
<td>64.0</td>
<td>89.1</td>
<td>68.4</td>
<td>95.2</td>
</tr>
<tr>
<td>Limit access to servers/applications</td>
<td>72.4</td>
<td>62.3</td>
<td>71.4</td>
<td>71.6</td>
<td>77.6</td>
<td>68.6</td>
<td>78.2</td>
<td>63.2</td>
<td>71.4</td>
</tr>
<tr>
<td>Timeout access</td>
<td>68.0</td>
<td>64.9</td>
<td>74.3</td>
<td>53.2</td>
<td>72.9</td>
<td>60.0</td>
<td>67.3</td>
<td>68.4</td>
<td>66.7</td>
</tr>
<tr>
<td>Recovery plan in case of disaster</td>
<td>48.5</td>
<td>50.0</td>
<td>54.3</td>
<td>45.9</td>
<td>54.1</td>
<td>35.3</td>
<td>41.8</td>
<td>52.6</td>
<td>33.6</td>
</tr>
<tr>
<td>Install closed desktop system</td>
<td>36.2</td>
<td>27.6</td>
<td>40.0</td>
<td>34.9</td>
<td>43.5</td>
<td>29.4</td>
<td>34.5</td>
<td>31.6</td>
<td>38.1</td>
</tr>
<tr>
<td>Limit URLs through firewall</td>
<td>30.5</td>
<td>17.6</td>
<td>20.0</td>
<td>28.7</td>
<td>32.9</td>
<td>33.3</td>
<td>43.6</td>
<td>33.3</td>
<td>38.1</td>
</tr>
<tr>
<td>Install directory inventory system to detect change</td>
<td>13.0</td>
<td>11.8</td>
<td>14.3</td>
<td>8.3</td>
<td>10.7</td>
<td>17.6</td>
<td>14.5</td>
<td>10.5</td>
<td>9.5</td>
</tr>
<tr>
<td>Use security devices for authentication</td>
<td>12.3</td>
<td>22.4</td>
<td>5.7</td>
<td>6.4</td>
<td>7.2</td>
<td>11.8</td>
<td>18.2</td>
<td>11.1</td>
<td>23.8</td>
</tr>
</tbody>
</table>
we found significant variations in adoption by institution size and type and between Carnegie categories. When compared with the private and business sectors, higher education lags in the installation of more advanced IT security technologies, but, as noted earlier, this may be due to different risk levels. We return to this topic in Chapter 10.

Endnotes


3. For a more detailed look at Gray’s views, see his “Network Security Credo” at <http://staff.washington.edu/gray/papers/credo.html>.

4. The Computer Crime and Security Survey is conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation’s Computer Intrusion Squad <http://www.goci.com/press/20030528.jhtml>. The survey, now in its eighth year, has the distinction of being the longest-running survey in the information security field. It is based on the responses of 530 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities.


5

Organization, Leadership, Policies, and Awareness

We begin this chapter with the hypothesis that institutions are still in the early stages of establishing an information technology (IT) security culture on campus. IT security is just beginning to gain a foothold in the day-to-day activities that govern an institution’s operations.

We also take the position espoused by the Government Accounting Office (GAO) that system security is a holistic problem, in which technological, managerial, organizational, regulatory, economic, and social aspects interact. We discussed technology in Chapter 4. We focus here on the human dimension of security and its foundation.

Managing IT Security on Campus

The Gramm-Leach-Bliley Act of 1999 as interpreted by the Federal Trade Commission in 2002 mandates that higher education institutions designate an individual to be responsible for IT security. The act doesn’t specify the person’s title, and the job doesn’t have to be full time; to whom the position reports is an internal institutional matter. Inevitably, this act will lead most if not all institutions to designate someone to be in charge of IT security. As a result, the numbers reported in this survey will change shortly. Our survey asked if someone had chief responsibility for IT security. We also asked about their title, when their position was created, their reporting relationships, and what skills and experience they had.

The vast majority of IT security leaders with day-to-day management responsibilities (96 percent) hold their position in the IT organization (see Figure 5-1). Directors of networking are most often in charge (31 percent), followed by chief IT security officers (22 percent) and CIOs (7 percent). The notable differences between Carnegie class institutions are the prominence of IT security officers at doctoral institutions and a greater role for academic management in Canada. Only 20 percent of the U.S. institutions surveyed have a full-time chief IT security officer. In Canada, however, 42 percent of institutions report having a full-time security officer. In the United States, 90 percent of the full-time security officers work at doctoral-extensive and doctoral-intensive institutions.

If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them.
—Henry David Thoreau
When Was the IT Security Position Created?

We asked respondents when their institution created the IT security officer position. The results (Figure 5-2) show a clear and steady pattern established in 1994. Canadian, baccalaureate, and master's institutions tended to create the position earlier than doctoral institutions.

Reasons for establishing an office varied. Philip Long, CIO at Yale University, noted that his university established a security office in conjunction with its enterprise resource planning (ERP) implementation. "When we installed our ERP project, it was a logical time to ask about security for a whole set of data that was coming online that hadn't necessarily been online. That was prior to year 2000. We went online in July 1999. We created the security office as an element of our IT system modernization going up to Y2K." South Dakota State University attributed its office in part to government and regulatory issues. At the North Dakota University System, it evolved informally after an outside auditor recommended formal policies and organization for IT security. At the University of Notre Dame, new leadership was a primary factor, as is often the case. For the Maricopa Community Colleges, the September 11, 2001, terrorist attacks were a major factor.

To Whom Does the IT Security Position Report?

Figure 5-3 shows that fully 95 percent of the IT security officers report to a senior administrator in the IT office, including 50 percent who report to the CIO. Only 5 percent report to academic or other non-IT senior managers. We found minor variations by Carnegie class. Approximately 20 percent of Canadian and associate's institutions report to other non-IT senior managers.
Figure 5-2. Creation of IT Security Position, by Year

Figure 5-3. To Whom Does the IT Security Officer Report?
These data are supported by the 2002 EDUCAUSE Core Data Service (CDS) survey, which shows that at 94 percent of 621 institutions, the IT security officer reports to another technology officer (Figure 5-4). Variation by Carnegie class is minimal.

At a CUMREC 2003 panel on IT security, the three panelists—Robert Clark, Jr., director of internal auditing at the Georgia Institute of Technology (Georgia Tech); Derek Kang, corporate compliance director at Shands HealthCare at the University of Florida; and Dan Updegrove, vice president for information technology at The University of Texas at Austin—expressed some difference of opinion regarding where to position the information security officer (ISO) in a higher education institution. Updegrove argued for the ISO’s reporting to the CIO: the ISO needs to be independent and partner with deans and others on campus. Kang saw the ISO’s reporting to the CIO as a potential conflict of interest, fearing the ISO would filter information, including budget information, given to the president and other senior managers. Clark thought both were right and said the question is how to create a reporting relationship that operates best on campus. At Georgia Tech, the ISO reports to the CIO, and the CIO and the internal auditor report regularly to the president, the board, and the vice president for finance.

From our in-depth interviews, we learned that Yale University has a dedicated security department with a “dotted-line report” to the auditing department head and a direct report to the CIO. The medical center has a separate organization with full-time security staff. At Indiana University, the Information Technology Policy Office and the Information Technology Security Office report directly to the vice president for information technology. According to Mark Bruhn, chief IT security and policy officer at Indiana University, “Policy and security responsibilities reside in the vice president’s office and do not report to the IT department, which signals the importance of keeping them out of areas with direct operational responsibilities.”

Figure 5-4. IT Security Officers Reporting to a Technology Officer
Certification

Numerous national security organizations and universities have organized formal IT security training programs that typically award a certificate upon successful completion of a course of study. Twelve percent (54) of the security managers in our survey have IT security certification. Of these, 33 hold the Certified Information Systems Security Professional certificate (CISSP), nine hold the Global Information Assurance Certification, five hold the Earned Security+ certificate, and three hold the Certified Information Systems Auditor certificate. More than half (28) of the recipients are at doctoral institutions. Forty-four institutions report having one staff member with certification, two report having two, three have three, five have four, and one institution reports having more than 10 certified staff members. Again, primarily the doctoral institutions report having certified security staff, although the institution with more than 10 certified staff members is in the Carnegie specialized class.

Andrew Conley, network security officer at South Dakota State University, commented on certification’s significance. Having certification is a basis for trust. It shows “we have gone through training and that we have this knowledge. I don’t think certification proves knowledge, but it is a qualifier that says you have put in time and the effort. It reassures the user base.” Martin Fraser, professor and chair of the computer science department at Georgia State University, agreed. “From the faculty perspective, certification does help—it lends credence and authority that can get the attention of academic units better. [It is] training that is acknowledged.”

Gary Dobbins, director of information security, University of Notre Dame, noted that each of their three security positions is certified. “We wrote that into the position descriptions as a requirement. We value the certification, and it has provided us with a direct benefit on more than one occasion. The certification requirement gave us knowledge in areas we might have otherwise been inclined to pay less attention to.”

William Carter, associate vice president for information technology at Austin Community College, gave a mixed review. “One of the problems that I have with certification is that when you finish with the program, your knowledge is out of date. You spend a lot of time taking follow-up courses. Your certification is good for a year afterwards and then your skills are outdated, unless you are using them all of the time. I think experience is more important—day-to-day working on a network is very different from what you learn in a class.”

The certification figures for higher education’s highest-ranking IT security staff are low, but they mirror some findings for industry. The 2002 KPMG survey found that 73 percent of security staff had no formal security qualifications, 8 percent had earned the CISSP certificate, 5 percent had university-accredited information security qualification, and 7 percent had security vendor certificates. This may be partially attributable to the certification programs’ relative newness.

Some campuses also offer their own security training. At Indiana University, for example, the Information Technology Security Office offers a certificate of completion for staff members who complete a series of classes called Security EdCert, specifically designed for local support providers who want to enhance their IT security knowledge.
Salaries

Figure 5-5 shows the IT security position salary range. Forty-three percent are paid in the range of $50,000–$74,999; 64 percent earn $75,000 or less. Salaries are generally higher in private institutions, with the highest salaries almost exclusively reported at doctoral institutions. No salary over $100,000 was reported in Canada. As we might expect, higher education does not compare favorably with industry here. In a study published by Information Security magazine in August 2002, the average salary for a “security manager” across both the public and private sectors was approximately $121,000, while the average for a “security director” was $154,000.1

We also looked at whether an institution’s number of networked devices affected salaries, but we found Carnegie class to be a better predictor (see Figure 5-6). For example, security staff at AA institutions with a large number of devices were paid less than staff at doctoral institutions with a similar number of devices.

Staffing

The 2002 EDUCAUSE CDS survey queried respondents on the size of their IT security staff. The mean number of full-time staff and full-time students are provided for each Carnegie class. Clearly the doctoral institutions employ the most IT security staff (see Figure 5-7).
Figure 5-6. IT Security Managers’ Salary Range, by Carnegie Class and Percentage of Institutions

Figure 5-7. Full-Time Student and IT Security Staff

Graphs showing salary ranges and percentage of institutions for IT security managers, and full-time student and IT security staff by Carnegie class.
The ECAR survey found that 50 percent of the institutions have full-time security staff (see Figure 5-8). Twenty-one percent have one full-time employee managing security, 12 percent have two employees, 3 percent have three employees, and 5 percent have six or more employees. While the doctoral institutions most often have multiple positions, it is interesting to note that every Carnegie class grouping has at least one institution with none, one, or multiple positions.

As the number of networked devices increases, so does the number of full-time staff, especially as the number of devices increases above 10,000. But we still found great variation by size, for reasons captured by The University of Texas at Austin’s Dan Updegrove. “I think it is a very complex model that we would have to develop to determine appropriate IT security staffing levels. You cannot automatically conclude that one campus with 40,000 computers needs twice as many security personnel as another campus with 20,000 computers. The larger campus may have a very uniform IT infrastructure, well-trained users and local system administrators, and locked-down desktops. This reduces the likelihood of problems, so the number of needed security personnel could be comparably modest. The smaller campus may conduct state-of-the-art research, use many domains, have no controls on the desktop, and have poorly trained users. Its exposure may be five times greater than the larger campus. It is extremely hard to get a handle on it.”

The 2002 KPMG survey found the number of full-time-equivalent (FTE) IT security staff to be roughly proportional to organization size, as measured by number of employees. We did not find the same level of proportionality when looking at enrollment and number of users and devices on the network, probably for many of the reasons Updegrove mentioned. But we did find a tendency for the larger institutions to employ more full-time staff.

**Staffing Trends**

We asked institutions whether they anticipated changes in the number of IT security employees within the next two years. Fewer than 1 percent (two institutions) indicated a staff decrease, while 66 percent expected no change, 25 percent expected to add one staff member, and 9 percent expected to add two or more. The anticipated increases are largely at doctoral institutions.

![Figure 5-8. Number of Full-Time Central IT Security Staff (N = 435)](image-url)
Yale’s Philip Long provided one interesting perspective on staffing trends. “If I received extra person or budget resources, I would not invest them in IT security. I would invest in critical IT infrastructure, and that helps with security. I don’t want more reactive resources; I want more proactive resources, by which I mean building infrastructure so good that the campus can avoid problems.”

Consultants
Outside consultants can supplement institutional staff’s efforts and expertise. They provide just-in-time expertise and complementary skills not otherwise available at the institution. Paul Howell, information systems security officer at the University of Michigan, uses consultants to upgrade firewalls. Otherwise, he says, “I would have to develop an expertise on upgrades. To me it is just cheaper to pay consultants to come in once a year and lead the upgrade effort than to have spare hardware and to devote time and energy to understanding the upgrade process.” Many schools have found consultants helpful in explaining the new HIPAA regulations.

Forty-one percent of institutions surveyed had used consultants for IT security–related services in the past 18 months. Of those that had, we asked what services they purchased or were considering. Table 5-1 provides the answers.

Table 5-1. Security Consultants and Services Used

<table>
<thead>
<tr>
<th>Consultant Service</th>
<th>Action (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Purchased</td>
</tr>
<tr>
<td>Managed incident response</td>
<td>1.1</td>
</tr>
<tr>
<td>Custom engineering</td>
<td>2.3</td>
</tr>
<tr>
<td>Manage projects</td>
<td>3.9</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>3.9</td>
</tr>
<tr>
<td>Manage VPN</td>
<td>4.4</td>
</tr>
<tr>
<td>Write policy</td>
<td>4.8</td>
</tr>
<tr>
<td>Manage antivirus service</td>
<td>5.1</td>
</tr>
<tr>
<td>Training and awareness</td>
<td>5.3</td>
</tr>
<tr>
<td>Managed firewall</td>
<td>6.4</td>
</tr>
<tr>
<td>Physical audit</td>
<td>6.7</td>
</tr>
<tr>
<td>Planning</td>
<td>8.3</td>
</tr>
<tr>
<td>Technical support</td>
<td>9.0</td>
</tr>
<tr>
<td>Architecture/design</td>
<td>9.9</td>
</tr>
<tr>
<td>Audit</td>
<td>10.8</td>
</tr>
<tr>
<td>Train IT staff</td>
<td>15.9</td>
</tr>
</tbody>
</table>
Clearly, higher education does not extensively use consultants for IT security services. We found their greatest use in training (16 percent), followed by IT security auditing (11 percent), design (10 percent), and technical support (9 percent). With the exception of the largest institutions’ hiring consultants slightly more often, we found no noticeable differences in use of consultants or type of service purchased attributable to Carnegie class, institution size, public versus private status, or country.

We asked those who used consultants to evaluate their performance using a five-point Likert scale: 1 is strongly agree, 2 is agree, 3 is neutral, 4 is disagree, and 5 is strongly disagree. The respondents were for the most part positive (see Table 5-2), expressing strongest agreement on consultants’ ability to provide technical expertise (mean of 2.08), product expertise (2.10), and insight from previous projects (2.19). Respondents generally agreed that the consultants helped meet project objectives, get more functionality from the security project, and meet the project timeline. Respondents were neutral on such items as meeting project budget and exceeding expected costs, and were gen-

Table 5-2. Assessment of IT Security Consultant Services

<table>
<thead>
<tr>
<th>Consultant Attribute</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide technical expertise not available internally</td>
<td>2.08</td>
<td>0.888</td>
</tr>
<tr>
<td>Provide product expertise not available internally</td>
<td>2.10</td>
<td>0.909</td>
</tr>
<tr>
<td>Brought insight from previous projects</td>
<td>2.19</td>
<td>0.828</td>
</tr>
<tr>
<td>Helped to achieve objective</td>
<td>2.29</td>
<td>0.854</td>
</tr>
<tr>
<td>Derive more value/function from security program</td>
<td>2.32</td>
<td>0.832</td>
</tr>
<tr>
<td>Value for money spent</td>
<td>2.36</td>
<td>0.869</td>
</tr>
<tr>
<td>Helped meet project timeline</td>
<td>2.67</td>
<td>0.913</td>
</tr>
<tr>
<td>No need for new FTEs</td>
<td>2.77</td>
<td>1.028</td>
</tr>
<tr>
<td>Provide project management not available internally</td>
<td>2.98</td>
<td>0.943</td>
</tr>
<tr>
<td>Helped meet project budget</td>
<td>2.99</td>
<td>0.849</td>
</tr>
<tr>
<td>Cost more than expected</td>
<td>3.10</td>
<td>0.914</td>
</tr>
<tr>
<td>Knowledge not transferred to staff</td>
<td>3.18</td>
<td>0.974</td>
</tr>
<tr>
<td>Did not understand higher education</td>
<td>3.20</td>
<td>1.033</td>
</tr>
<tr>
<td>Experience overstated</td>
<td>3.23</td>
<td>0.997</td>
</tr>
<tr>
<td>Personnel not a good fit</td>
<td>3.39</td>
<td>0.839</td>
</tr>
<tr>
<td>Did not work well with internal resources</td>
<td>3.56</td>
<td>0.754</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)
erally positive on knowledge transfer and ability to work with internal sources. Note that these latter questions were stated in the negative; therefore, the higher mean (three or higher) is the more positive response.

We compared the means and found no noticeable differences attributable to Carnegie class, institution size, public versus private status, or country. Baccalaureate and associate’s institutions were slightly more positive about consultants’ supplementing internal expertise, which is not surprising because these institutions have, on average, fewer staff than doctoral institutions.

**IT Security Organization**

The IT security literature recommends the establishment of a central security office. At an August 2002 NSF workshop in Chicago organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force, participants identified establishing a centralized security organization as the highest priority agenda item in the area of security organization. James Wright, president of Dartmouth College, asserted that “security must be a centralized function, and all functional managers must understand that variance from the campus standard in this area is not an option.”

**Advantages of a Central Security Office**

The GAO, in its May 1998 *Executive Guide, Information Security Management, Learning from Leading Organizations*, indicated that central security offices can help the institution by

- serving as catalysts to ensure that information security risks are considered in both planned and ongoing operations;
- providing advice and expertise to units throughout the institution;
- keeping top management informed about security-related issues and activities affecting the organization;
- achieving some efficiency and increasing consistency in the organization’s security program implementation by performing tasks centrally that multiple individual business units might otherwise perform;
- providing training;
- researching potential threats, vulnerabilities, and control techniques and communicating this information to others in the organization;
- monitoring various aspects of the organization’s security-related activities by testing controls, accounting for the number and types of security incidents, and evaluating compliance with policies;
- establishing a computer incident response capability and, in some cases, serving as members of the emergency response team;
- assessing risks and identifying needed policies and controls for general support systems, such as organization-wide networks or central data-processing centers;
- creating standard data classifications and related definitions to facilitate protection of data shared among two or more business units;
- reviewing and testing the security features in both commercially developed software being considered for use and internally developed software prior to moving it into production; and
- providing self-assessment tools to business units to let them monitor their own security posture.

Our data confirm the GAO’s assertion. Institutions with a dedicated security staff will much more likely fulfill the above functions.
Centralized and Decentralized Security Offices

Our interview data provided examples of organizational structures. Indiana University (IU) established two distinct offices: the Information Technology Policy Office (ITPO) and the Information Technology Security Office (ITSO). These offices are intentionally distinct: the ITPO handles IT policy development, dissemination, and education, and the ITSO handles security analysis, development, education, and guidance for IU’s information assets and IT environment.

While not splitting security into distinct offices, several institutions we interviewed already segment, or plan to segment, functions within the security organization to focus on either technology versus policy or academic versus administrative security issues. For example, South Dakota State University plans to split their chief security officer position into two, one with a technical focus and the other with a culture interface/awareness focus. Yale University has two functional areas in their security office: one technician focuses on administrative security issues and the other on academic security issues.

The quantitative data in Figure 5-9 reflect that 57 percent of institutions spread IT security across multiple functional areas; only 11 percent have a dedicated IT security staff. At 22 percent of the institutions, IT security is the responsibility of a single individual. Two institutions outsourced their IT security.

As Figure 5-10 illustrates, we found 50 percent of the dedicated IT security staff offices at doctoral institutions and 90 percent at doctoral, system, and specialized institutions (notably medical schools).

Security Policy

According to the GAO, “The framework within which an organization strives to meet its needs for information security is codified as security policy. A security policy is a concise statement, by those responsible for a system (such as senior management), of information values, protection responsibilities, and organizational commitment.”

Scott Blake of BindView Corp. and Patrick McBride of the META Security Group stated that a security policy provides a framework for:

- making consistent, timely, and cost-effective management decisions;
- selecting security controls and products;
- defining and empowering acceptable behavior [by students, faculty, and staff]; and
- empowering [members of the institution’s community to do their work] securely.

A security policy can also establish goals. Gordon Wishon, CIO of the University of Notre Dame, said, “The primary goals at this time are, one, to address liability for the university—legal and civil liability that results from a mishandling and/or misappropriation of protected information; two, a secondary but almost equal concern is the effort, energy, cost, and expense of dealing with incidents and clean up from viruses; and three, the concern that we have for students and faculty and protecting them from some of the negative effects of life on the Internet.”

Indiana University’s Mark Bruhn explained, “Institutional values drive policy; policy dictates processes, procedures, and standards; and security implements those.” We would elaborate on Bruhn’s astute observation. Several IT security commentators have expressed concern that IT security can be inimical to academic freedom, but we believe this depends on the policy driving IT security at a particular institution and not on the tools themselves. Indeed, IT security can support academic freedom by ensuring
ready and timely access to information by authorized users. This is a major reason for having a comprehensive IT security policy: it can embed the academy’s most important values into an area that some might otherwise find problematic. We elaborate on this topic in Chapter 10.

Moreover, IT security policy is critical to holding all parties in the institution accountable. As Blake and McBride point out, “Because security measures are disaster-preventing rather than payoff-producing, a central aspect of security must be accountability. That is, users and operators must be
held responsible by management for taking all appropriate security measures. One cannot count on financial and market incentives alone to drive appropriate action. Many security problems exist not because a fix is unknown, but because some responsible party has not implemented a known fix." A good security policy can play an important role in liability abatement by demonstrating that the institution has taken appropriate and necessary precautions to protect its information assets and clients.

Campus Policies
Where and when have security policies been implemented? Who was involved in their development? What policies have institutions put into place regarding access to and usage of their networks, computing resources, applications, and data or information resources? Are these policies enforced and updated? What reactions, if any, did these policies generate on campus? What emerging issues are forcing policy changes? How are institutions reacting?

Fifty-four percent (235) of the institutions queried indicated that they have a formal institutional policy (or policies) covering IT security (see Table 5-3). Nineteen percent of the 235 institutions with formal policies also had interim policies or were implementing additional policies. Twenty-three percent of respondents had no formal policy but did have an interim policy; an additional 15 percent were implementing a formal policy. Only 8 percent had no policy, formal or interim.

Figure 5-11 shows that institutions are steadily putting in place formal IT policies. Table 5-4 indicates which security areas the formal policies cover for all institutions and by Carnegie class. Virtually all policies address appropriate use of institutional assets, and 80 to 90 percent of policies cover system access control, authority to shut off Internet access, data security, network security, enforcement of institutional policies, and desktop security. Policies less often address physical security of assets, residence halls, remote devices, and application development.

Table 5-3. IT Security Policies in Place

<table>
<thead>
<tr>
<th>Status of Policies</th>
<th>Number of Institutions</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implemented, interim, and implementing</td>
<td>45</td>
<td>10.3</td>
</tr>
<tr>
<td>Implemented and interim policies, not implementing</td>
<td>13</td>
<td>2.9</td>
</tr>
<tr>
<td>Implemented, no interim, implementing</td>
<td>24</td>
<td>5.5</td>
</tr>
<tr>
<td>Implemented, no interim, not implementing</td>
<td>153</td>
<td>35.2</td>
</tr>
<tr>
<td>No formal policy, have interim, are implementing</td>
<td>39</td>
<td>9.0</td>
</tr>
<tr>
<td>No formal policy, have interim, not implementing</td>
<td>62</td>
<td>13.7</td>
</tr>
<tr>
<td>No formal policy, no interim, are implementing</td>
<td>64</td>
<td>14.7</td>
</tr>
<tr>
<td>No formal policy, no interim, not implementing</td>
<td>35</td>
<td>8.0</td>
</tr>
</tbody>
</table>
Table 5-4. What Do the Policies Cover? Differences by Carnegie Class and Canada

<table>
<thead>
<tr>
<th>What Formal Policies Cover</th>
<th>Positive Response, by Carnegie Class (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All</td>
</tr>
<tr>
<td>Appropriate use of institutional assets</td>
<td>99</td>
</tr>
<tr>
<td>System access control</td>
<td>89</td>
</tr>
<tr>
<td>Authority to shut off Internet access</td>
<td>85</td>
</tr>
<tr>
<td>Data security</td>
<td>83</td>
</tr>
<tr>
<td>Network security</td>
<td>82</td>
</tr>
<tr>
<td>Enforcement of institutional policies</td>
<td>82</td>
</tr>
<tr>
<td>Desktop security</td>
<td>80</td>
</tr>
<tr>
<td>Physical security of assets</td>
<td>71</td>
</tr>
<tr>
<td>Residence halls</td>
<td>61</td>
</tr>
<tr>
<td>Remote devices</td>
<td>51</td>
</tr>
<tr>
<td>Application development</td>
<td>39</td>
</tr>
</tbody>
</table>
policies, but note that at many institutions included in the study, residence halls and remote devices are not available and application development is not undertaken.

We found some differences among Carnegie classes. Doctoral-intensive and baccalaureate institutional policies are more likely to exceed the average coverage for all areas, and doctoral-extensive and Canadian policies are less likely to exceed the average. Small institutions’ policies more likely exceed the average on desktop security. There was very little difference between private and public institutions, with the exception of application development (41 percent “yes” at public institutions and 29 percent “yes” at private institutions). Private institutions’ policies were more likely to cover residence halls (72 percent versus 51 percent for public), but that may be attributable to the very low number of residence facilities at AA institutions (only 8 percent have residence halls), which are mostly public (48 of 51) in this study.

Specificity varies, too. The North Dakota University System segments their security policies into five areas: network security, data security, desktop security, physical security, and system security. Philip Long, CIO, said Yale University has “an overall appropriate use policy that makes it clear that anything that threatens the network is prohibited and that any misbehaving machine will be disconnected. We do not have a policy that goes into detail—you may not run a machine that is compromised with a virus, etc. Rather we have general language that any IT action that is impeding the community is prohibited. Then, we use, in theory, good judgment.”

**Security Policy Characteristics**

Security policies must be easy to read, accessible, enforced, comprehensive in scope, regularly updated, and consistent across the institution. We asked respondents to assess their institution’s IT security policies on each of these dimensions. Table 5-5 shows the mean value and standard deviation for each characteristic in rank order. The mean is based on a four-point Likert scale: 1 is strongly agree, 2 agree, 3 disagree, and 4 strongly disagree.

There is stronger disagreement about policies being regularly updated and comprehensive. A few institutions men-

<table>
<thead>
<tr>
<th>Policy Characteristic</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies are accessible</td>
<td>1.92</td>
<td>0.708</td>
</tr>
<tr>
<td>Policies are clear and easy to read</td>
<td>1.98</td>
<td>0.583</td>
</tr>
<tr>
<td>Policies are consistent across the institution</td>
<td>2.08</td>
<td>0.748</td>
</tr>
<tr>
<td>Policies are enforced</td>
<td>2.09</td>
<td>0.659</td>
</tr>
<tr>
<td>Policies are regularly updated</td>
<td>2.44</td>
<td>0.717</td>
</tr>
<tr>
<td>Policies are comprehensive</td>
<td>2.53</td>
<td>0.798</td>
</tr>
</tbody>
</table>

*Scale = 1 (Strongly Agree) to 4 (Strongly Disagree)*
tioned that they avoided updating policies because of an arduous approval process. Our respondents ranked the characteristics “accessibility” and “easy to read” highest among the six characteristics. We also looked for differences between public and private institutions and between Carnegie classes, as well as differences by institution size. Respondents from private institutions ranked all policy characteristics more favorably than did those from public institutions, but only by a very small amount. Otherwise, differences were minor and not significant.

Indiana University emphasized the need for easy-to-understand security policies. “Policies must be easy to read, understand, and interpret,” emphasized Merri Beth Lavagnino, deputy IT policy officer. “Even though we have foundation policies, it’s very difficult for the person who doesn’t work with them every day to understand them. These folks call Mark [Bruhn] or me. We need to work on education and awareness. I’d love to spend more time in making policies more accessible—maybe have an ‘ask the policy guy’.” Bruhn agreed. “We need and want the formal policies to exist, but also need another format that makes them easier to read, less formal, and more narrative.”

**Leadership’s Involvement in Policy Development**

The best-practice literature on policy development encourages senior management’s active engagement, not simply their support or endorsement. Dartmouth College President James Wright said, “Privacy and academic freedom are critical components of campus culture; it is vital that decisions on policies and practices regarding security and related issues be carefully vetted, understood, and authorized by both the highest levels of the campus leadership and the representatives of the campus community. The executive role in all of these matters is crucial if internal dissention and unnecessary strife are to be avoided.”

Georgia Tech’s Robert Clark, Jr. advised attendees at the CUMREC 2003 Security Panel, “If you’re asked to develop policies, don’t do it on your own. It is a shared responsibility. At Georgia Tech we have a committee with legal, audit, vice president for human resources, vice president for finance, an assistant dean, student, CIO, and director of information security. First do an evaluation and assessment of risk. Assess the degree of risk at the institutional level. Often the risk is being assumed by default rather than thinking about it—it is not up to the individual units to decide. Raise the visibility of security so that the president makes the decision.”

When Michael McRobbie, Indiana University’s vice president for information technology and CIO, came to IU in January 1997, he immediately established a good working relationship with then-president Myles Brand. Brand became a strong advocate for IU’s security efforts. This executive-level support enabled IU to proceed more quickly in adopting security policies and practices than it could have without this support. Because IT security is very much a cultural issue, the leaders who can most effectively change the institution’s culture must be visible and engaged.

Also important for changing the culture are the governance groups. In a May 2003 presentation to the Common Systems Group, Jack McCredie, CIO of the University of California, Berkeley, recommended, “The policy development process should include engaging the IT governance structure for collaboration and policy formulation, providing opportunity for input throughout the development process, soliciting
input from non-IT committees, obtaining approvals from senior management, and communicating, communicating, communicating.”

James Wright of Dartmouth suggested that “with security issues, the parties that may need to be involved are potentially quite different from those that were involved in past years.” IT security impinges on ethical and philosophical issues, on teaching and research as well as on most business areas, and it goes beyond a single college or unit.

Data on Leadership Involvement

We asked our respondents about their senior management’s level of involvement in developing their institution’s security policies (see Table 5-6). We calculated the mean and standard deviation for each administrator, office, or agency on the basis of a five-point Likert scale.

We found the most agreement and the least difference of opinion on the active engagement of the IT organization and the CIO. Senior academic officers, the board, and external state agencies are not seen as having anywhere near as much involvement in IT security policy development.

We also looked for differences based on public versus private institution, institutional size, and Carnegie class. Overall, we found few differences and nothing of statistical significance. Those at private institutions see the board and president as less involved than do respondents at public institutions. Senior administrators other than the CIO are seen as more involved at AA institutions, probably because there are fewer CIOs at these institutions. The faculty and internal auditor were more engaged at doctoral and larger institutions. And Canadian institutions mirrored their American counterparts across the board.

Table 5-6. Participants in the Development of IT Security Policy, Ranked by Level of Participation

<table>
<thead>
<tr>
<th>Participation</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Organization</td>
<td>1.74</td>
<td>0.726</td>
</tr>
<tr>
<td>CIO</td>
<td>2.06</td>
<td>0.977</td>
</tr>
<tr>
<td>Campus/Faculty Task Force</td>
<td>2.89</td>
<td>1.262</td>
</tr>
<tr>
<td>System Office</td>
<td>3.10</td>
<td>1.245</td>
</tr>
<tr>
<td>Internal Auditor</td>
<td>3.31</td>
<td>1.149</td>
</tr>
<tr>
<td>Provost</td>
<td>3.48</td>
<td>1.160</td>
</tr>
<tr>
<td>External Auditor</td>
<td>3.58</td>
<td>1.094</td>
</tr>
<tr>
<td>President</td>
<td>3.67</td>
<td>1.035</td>
</tr>
<tr>
<td>Board of Trustees</td>
<td>3.90</td>
<td>0.927</td>
</tr>
<tr>
<td>State Agency</td>
<td>4.03</td>
<td>1.012</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)
The Leadership Challenge

Our data suggest that a concern for IT security has not been adequately carried forward to the executive level. An executive vice president of a large research university confirmed this view when asked about his level of involvement with IT security. He replied, “That is mostly left to the technology folks and to the CIO, at the vice president level. Most other executives aren’t deeply involved, except at the medical center.”

One reason for their lack of interest may be that historically, IT security breaches, when they have occurred, haven’t impacted the institution, or the executives themselves, as much as other incident types. For example, we found no documented instances of a university executive losing his or her job over an IT security breach, whereas incidents such as financial fraud and athletics scandals have brought down university administrations.

Awareness

Is the campus community well educated about security risks? Are awareness programs and practices in place, if so for whom, and are they effective? The issue is critical, as many believe that the greatest risk to the institution is internal. While most internal users are not ever going to try to maliciously compromise the institution’s systems, many security issues arise when an internal user inadvertently compromises security, for example, by not installing an operating system patch or by giving their password to someone over the phone. The 2003 Healthcare Information and Management Systems Society Leadership Survey indicated that an internal security breach was the primary threat to their organizations (55 percent of the respondents). External threats scored 23 percent. Gregory Jackson, vice president and CIO at the University of Chicago, said his “biggest concern is that a very large portion of the people who connect to the network have no concept of security and [are] showing up with improper setups.”

Continuous security education is likely one of the most cost-effective and important defensive strategies an institution can take, and several helpful Web sites offer good ideas. At the NSF Security Architecture and Policy Workshop in August of 2002 in Chicago, attendees asked to rate priorities for an action agenda cast the most votes (34) for a campus-wide security awareness campaign. They also highly supported sharing training materials across campuses (21 votes), developing security training and education courses for staff and faculty (20 votes), and building awareness among higher education executives regarding security issues and risks (16 votes). Notre Dame’s Gordon Wishon noted the importance of awareness: “The lack of attention to security is a long-standing situation and has led to a huge awareness gap. We should invest in a very high degree of awareness. Awareness building does not have to cost a lot of money, but it definitely needs attention.” Our data show the priority is a pressing one, as awareness programs on many campuses are not as strong as Wishon and the authors believe they should be.

Kim Milford, information security manager at the University of Wisconsin–Madison, emphasized the importance of building campus security awareness. “One important area of awareness that we’ve developed is an annual security conference, called Lockdown,” she said. “UW–Madison system administrators, IT staff from other University of Wisconsin institutions, and IT staff from state agencies attended this two-day conference. We bring in regional and national speakers to discuss current security issues, such as legal considerations, risk assessment, and Microsoft security. The content includes both technical and policy topics. It provides a great opportunity to get campus
system administrators together to discuss security as well as increase their education and awareness.”

**IT Security As a Campus Priority**

We asked the respondents whether IT security was one of the top three issues confronting their institution today. Seventy-five percent agreed or strongly agreed that it was, 15 percent were neutral, and 10 percent disagreed or strongly disagreed. Respondents who strongly agreed were most likely to come from large doctoral institutions. We also asked whether IT security was a priority of their institution. Sixty-one percent agreed or strongly agreed that it was, 25 percent were neutral, and 14 percent disagreed or strongly disagreed. The mean on a scale of 1 to 5 (1 is strongly agree, 2 agree, 3 neutral, 4 disagree, and 5 strongly disagree) was 2.39. Again, respondents who strongly agreed were most likely to come from large doctoral institutions.

**Reporting**

We asked how often IT security was discussed at the president’s or chancellor’s cabinet meetings and how often the IT security office made a report to senior management on IT security. Fewer than 1 percent said it was very often discussed at cabinet meetings, 10 percent said often, 29 percent occasionally, 29 percent seldom, and 9 percent never. One-quarter of the respondents answered “don’t know.” For reporting, the percentages were higher, with 3 percent saying very often, 14 percent often, 37 percent occasionally, 31 percent seldom, and 15 percent never. Eight percent did not know. Institutions reporting “never” were most often small, with 2,000 or fewer enrolled students.

Table 5-7 shows the periodicity of reporting to senior management, by Carnegie class. We found reporting to be more likely at doctoral institutions. However, in light of best practices, these numbers are low. Not surprisingly, for institutions that had an

<table>
<thead>
<tr>
<th>Carnegie Class</th>
<th>Reports to Senior Management (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Often</td>
</tr>
<tr>
<td>Dr. Ext.</td>
<td>2.7</td>
</tr>
<tr>
<td>Dr. Int.</td>
<td>–</td>
</tr>
<tr>
<td>MA</td>
<td>4.0</td>
</tr>
<tr>
<td>BA</td>
<td>1.3</td>
</tr>
<tr>
<td>AA</td>
<td>2.3</td>
</tr>
<tr>
<td>Specialized</td>
<td>2.0</td>
</tr>
<tr>
<td>System</td>
<td>6.7</td>
</tr>
</tbody>
</table>
incident reported in the press, the reporting level was higher.

We did a means comparison on reporting and looked at Carnegie class (Table 5-8). The lower the mean, the more often reports were made to senior management (1 is very often and 5 is never).

The number of devices proved to be the better predictor. The more devices on the network, the more often reports were made (see Table 5-9).

Indiana University’s president and board of trustees have clearly made IT security a priority. Through regular briefings and discus-

<table>
<thead>
<tr>
<th>Carnegie Class</th>
<th>Mean</th>
<th>N</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Ext.</td>
<td>3.15</td>
<td>74</td>
<td>0.917</td>
</tr>
<tr>
<td>Dr. Int.</td>
<td>3.32</td>
<td>31</td>
<td>0.945</td>
</tr>
<tr>
<td>MA</td>
<td>3.50</td>
<td>101</td>
<td>1.036</td>
</tr>
<tr>
<td>BA</td>
<td>3.70</td>
<td>79</td>
<td>1.005</td>
</tr>
<tr>
<td>AA</td>
<td>3.47</td>
<td>43</td>
<td>0.984</td>
</tr>
<tr>
<td>Specialized</td>
<td>3.58</td>
<td>50</td>
<td>0.971</td>
</tr>
<tr>
<td>System</td>
<td>3.07</td>
<td>15</td>
<td>1.033</td>
</tr>
<tr>
<td>Total</td>
<td>3.45</td>
<td>393</td>
<td>0.999</td>
</tr>
</tbody>
</table>

Table 5-8. Mean Frequency Reporting to Senior Management by Carnegie Class

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Mean</th>
<th>N</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 1,000</td>
<td>3.63</td>
<td>64</td>
<td>0.864</td>
</tr>
<tr>
<td>1,001–5,000</td>
<td>3.56</td>
<td>168</td>
<td>1.031</td>
</tr>
<tr>
<td>5,001–10,000</td>
<td>3.63</td>
<td>67</td>
<td>0.967</td>
</tr>
<tr>
<td>10,001–20,000</td>
<td>3.00</td>
<td>45</td>
<td>1.044</td>
</tr>
<tr>
<td>20,001–40,000</td>
<td>3.10</td>
<td>21</td>
<td>0.889</td>
</tr>
<tr>
<td>40,001–60,000</td>
<td>3.17</td>
<td>12</td>
<td>0.835</td>
</tr>
<tr>
<td>60,001–80,000</td>
<td>2.60</td>
<td>5</td>
<td>0.548</td>
</tr>
<tr>
<td>More than 80,000</td>
<td>2.50</td>
<td>4</td>
<td>0.577</td>
</tr>
<tr>
<td>Not Centrally</td>
<td>3.00</td>
<td>6</td>
<td>0.894</td>
</tr>
<tr>
<td>Total</td>
<td>3.45</td>
<td>392</td>
<td>1.000</td>
</tr>
</tbody>
</table>

Table 5-9. Reporting to Management by Number of Network Devices
essions with McRobbie, the board has come to understand the risks to the institution of poor security. After a security breach resulting in the release of personal information from the Office of the Bursar in early 2001, the board voted to quantify and strengthen the vice president of information technology and CIO’s responsibility with a resolution that the office assume leadership, responsibility, and control of responses to unauthorized access to IU’s IT infrastructure.

We asked respondents if IT security practices were woven into the institution’s business practices. The majority (58 percent) were neutral or negative. On a Likert scale of 1 to 5, the mean value for the respondents was 2.89. Doctoral-intensive institutions did best, but on the whole we found little difference among institutions of varying size or Carnegie class, and between public versus private or United States versus Canada.

We did see more variation when asking whether “IT security problems inadvertently caused by authorized users are significant.” A majority agreed or strongly agreed that this was a problem. On a Likert scale of 1 to 5, the mean value for the respondents was 2.59, which suggests a fairly even divide. Larger schools and doctoral institutions were more likely to see it as a problem. The University of Texas at Austin provides a good example: the SQL Slammer worm was under control until an MBA student came to campus and plugged in an infected laptop inside the firewall. Clearly, it is a challenge for the ordinary user to learn about ports, time limits, advisories, and so on.

The dilemma here is that people take security for granted. We know that many deans or directors provide their personal assistants with their user IDs and passwords for reading their e-mail. Such behavior, while understandable at one level, nevertheless suggests a serious vulnerability to their other personal information and access privileges. Awareness programs are key to improving IT security behavior.

**Awareness Programs**

Surprisingly, only one-third of the institutions had a formal awareness program for students and faculty (see Figure 5-12). Only slightly more—39 percent—had a formal awareness program for staff. Again, we found some differences by Carnegie class: doctoral institutions were more likely to have awareness programs. We found no differences between public versus private or Canadian versus American institutions.

Doctoral institutions, which are more likely to have a dedicated IT security staff, are also therefore more likely to have formal awareness programs (Figure 5-13). Also, the larger the dedicated IT security staff, the more likely there will be a formal awareness program.

Numerous institutions have developed security awareness programs as part of student orientation. At Embry-Riddle Aeronautical University, for example, a formal training program for students called Back to School explains to students and their parents their rights and responsibilities. Students go through a half-hour program during orientation before they receive their PINs and passwords.

Doug Kankel, professor of molecular, cellular, and developmental biology at Yale University, evaluated the level of faculty awareness: “I would say that faculty-wide awareness is not high. The awareness level probably scales in some way with the so-
Figure 5-12. Awareness Programs, by Carnegie Class

Figure 5-13. Awareness Programs, by Type of IT Security Organization
phistication of the user and the specific demand. People who are running servers that are in fact reaching a larger set of individuals are probably more aware than individuals that are simply using a personal machine attached to the campus network. The further away one is from more sophisticated computing, the less one is aware of what the issues are.”

Creativity is also important to building security awareness on campus. “We’ve gone beyond just using Web announcements, newsletters, and e-mail—we’re creative with our awareness efforts, using such mediums as radio ads, videos, posters, and even putting messages on campus ATM machines,” said University of Wisconsin–Madison’s Kim Milford. “Often the statistics from our incident response team feed into our awareness efforts. The areas of largest concentration of incidents, such as copyright infringement, become the areas in which we focus our awareness efforts. We also get students to assist in developing our awareness programs, such as student creation of security videos. We find they understand the student audience better than we do.”

Information Week’s 2002 Global Information Security Survey indicates that only 27 percent of U.S. companies have conducted security training. Our data show slightly better performance by higher education. The percentages are disappointing, as this is one area where increased expenditure and effort could have an enormous payback to the institution. Security is much more than firewalls and antivirus tools. It is not obtained simply through the purchase of new technologies.

Effectiveness of Awareness Programs

When asked how effective the respondents felt their awareness programs had been, 70 percent were neutral or negative about the programs for their students and faculty (mean of 2.97 for students and 2.93 for faculty on a scale of 1 to 5, where 1 is strongly agree and 5 is strongly disagree), and 60 percent were neutral or negative for staff (mean of 3.78). There was little difference based on institution size, Carnegie class, public versus private status, or Canada versus the United States.

Andrew Conley of South Dakota State University provided a typical assessment of an institution’s awareness programs: “I’d say that the majority of faculty and staff are not aware of the policies, even though they are published on the Web. Some actions we are contemplating include a banner that pops up whenever a user logs in to a computer, stating that he or she agrees to the acceptable use policy and pointing the user to a site to view the policy. And also, we want to create a Web site and make everyone visit it and sign off with some sort of digital signature saying that they have agreed to it. The students are probably more aware of policies than the faculty because they have a small, short executive summary of the policy that they have to sign before they get Internet access.”

Budget

We asked respondents about the percentage of the central IT budget dedicated to IT security, and we present the range and answers in Figure 5-14. Of the respondents who provided data for this question, 55 percent spent from 1 to 5 percent of their central IT budget on security, and 14 percent spent 6 to 10 percent. Twenty-eight percent spent less than 1 percent. The 2002 EDUCAUSE CDS survey found that, on average, 86 percent of IT security funds came from the operating budget, 6 percent from the capital budget, and, at doctoral institutions, 10 percent from indirect cost recovery.
We had anticipated that the larger the institution, the smaller the percentage of its budget that would be spent on IT security. That is the reported case for private industry (Information Week's 2002 Global Information Security Survey). Information Security magazine's 2002 survey of 2,196 IT security practitioners showed that the larger the organization, the less it spends on security per user and per device. But we found no differences in the percentage of budget support among institutions of varying size, Carnegie class, public versus private status, or United States versus Canada. Information Security magazine's survey estimated that education spends about 4 percent of the IT budget for security, which is very close to our findings. These comparison figures might be misleading because many higher education institutions may spend a significant amount of money on IT security outside of the central IT organization, which would make the comparison numbers more favorable.

Universities spend less on security than government, banking, telecommunications, and other industries reportedly spend. According to Information Week's 2002 Global Information Security Survey, fielded by PriceWaterhouseCoopers, businesses spend on average 12.4 percent of their overall IT budget on IT security. The same survey indicated that education spent about 10 percent, but our numbers do not corroborate their findings. KPMG asked businesses how much of the IT budget was spent on security last year and whether it will be increased or decreased next year. They found that the average spent on IT security was USD$2.6 million, an average of 10.1 percent of the IT budget.
Future Spending
We then asked about changing expenditure patterns for IT security over the next 12 months. Table 5-10 presents the data.

Respondents expected training and hardware and software expenditures to increase more than staffing and external services, which almost two-thirds of the respondents thought would stay the same. Although they saw no difference for external services, the large-enrollment and doctoral institutions expected some increases in expenditures for staffing, training, and hardware and software. The numbers for higher education are slightly higher than the anticipated increases indicated by 3,000 randomly selected CIOs who participated in the 2003 CIO Magazine Tech Poll, which included business and higher education. The poll also revealed that security software is the strongest sector, with 52 percent of the respondents planning to increase spending.

<table>
<thead>
<tr>
<th>Change in Expenditure</th>
<th>Staffing</th>
<th>Hardware/Software</th>
<th>Training</th>
<th>External Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant increase</td>
<td>2.6</td>
<td>9.0</td>
<td>5.4</td>
<td>2.5</td>
</tr>
<tr>
<td>Some increase</td>
<td>25.6</td>
<td>38.7</td>
<td>37.0</td>
<td>19.2</td>
</tr>
<tr>
<td>About the same</td>
<td>63.3</td>
<td>40.1</td>
<td>43.9</td>
<td>62.3</td>
</tr>
<tr>
<td>Some decrease</td>
<td>7.6</td>
<td>10.6</td>
<td>11.1</td>
<td>12.3</td>
</tr>
<tr>
<td>Significant decrease</td>
<td>9.0</td>
<td>1.7</td>
<td>2.6</td>
<td>3.7</td>
</tr>
</tbody>
</table>

Sufficiency of Security Funding
We asked respondents whether their institution has provided the needed resources to address IT security issues, using a Likert scale of 1 to 5. Table 5-11 summarizes the results. The largest percentage thought the institution had not and therefore disagreed (33 percent); a total of 44 percent disagreed or strongly disagreed, 27 percent were neutral, and 28 percent agreed or strongly agreed. The differences among Carnegie classes were small, but college and university system offices and doctoral-intensive institutions expressed the most need.

Finally, we asked for the primary reason the institution uses to justify IT security expenses. Figure 5-15 shows the answers.

In order of frequency are strategic investment (21 percent), incident prevention (17 percent), and reaction to a major incident (16 percent). Small colleges more often mentioned reaction to a major incident, whereas doctoral institutions more often mentioned strategic investment. It may be that the ability to secure significant additional funding at small colleges depends, in part, on a reaction to a negative event. We also found that institutions with dedicated security staff were most likely to justify expenditures as major investments. This may explain the higher results for doctoral institutions.
Table 5-11. Level of Respondent Agreement on Whether IT Security Funding Is Sufficient, by Carnegie Class and United States Versus Canada

<table>
<thead>
<tr>
<th>Carnegie Class and Canada</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Ext.</td>
<td>3.28</td>
<td>0.947</td>
</tr>
<tr>
<td>Dr. Int.</td>
<td>3.43</td>
<td>1.065</td>
</tr>
<tr>
<td>MA</td>
<td>3.31</td>
<td>1.136</td>
</tr>
<tr>
<td>BA</td>
<td>3.10</td>
<td>1.020</td>
</tr>
<tr>
<td>AA</td>
<td>3.20</td>
<td>1.030</td>
</tr>
<tr>
<td>Specialized</td>
<td>3.25</td>
<td>1.031</td>
</tr>
<tr>
<td>System</td>
<td>3.42</td>
<td>1.071</td>
</tr>
<tr>
<td>Canada</td>
<td>3.23</td>
<td>1.044</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)
Endnotes


3. For a brief summary of the contents of a security policy, see ISO 17799:2000, p. 2.


5. Ibid.


7. Ibid., p. 45.

8. See <http://www.sans.org/resources/mistakes.php> for common mistakes that organizations can avoid through education.
In this chapter we address how the effective use of security technologies depends on information technology (IT) security practices. We pay particular attention to security planning, risk assessment, updating and maintaining systems, password use, monitoring, and the detection of threats. Installing technology is no guarantee that it will work; much depends on how, when, and where it is used, by whom, and with what level of effort and skill.

Security Planning

Institutions can be proactive or reactive with respect to security. One measure of a proactive security strategy is the preparation of an IT security plan that is comprehensive, in place, and followed.

We asked our respondents whether their institution had developed and adopted an IT security plan (see Figure 6-1). Thirteen percent reported that a comprehensive plan was in place at their institution; 10 percent said...
no IT security plan was in place. Forty-two percent had a partial plan in place, while 36 percent were currently developing a plan.

Table 6-1 shows the breakdown by Carnegie class, which did not reveal much variation. Further analysis shows only minor differences in IT security plan adoption between large-enrollment and small-enrollment institutions. However, IT organization does have an impact. Where responsibility for IT security is spread across the institution, a security plan is less likely to be in place. More positively, institutions with a dedicated security staff will more likely have a plan in place. We return to the importance of this latter factor in Chapter 8.

**Risk Assessments and Audits**

A risk assessment helps an institution determine its security requirements. According to ISO/IEC 17799:2000, the risk assessment should estimate the harm to business likely to result from a security failure causing a loss of information confidentiality, integrity, or availability. It should also estimate the likelihood of a failure occurring given the current threat environment and the controls currently in place at the institution. Periodic reviews are necessary to accommodate changes to the institution’s academic activities and business operations, to account for new threats and vulnerabilities, and to confirm that current controls are effective and operative. A risk assessment differs from a vulnerability assessment, which identifies errors or weaknesses in system design, implementation, or operation. A threat is an adversary motivated to exploit a system’s vulnerability and capable of doing so. In summary, risk refers to the likelihood that system vulnerabilities will be exploited or that a threat may become harmful.

Thirty percent of the institutions in our study had undertaken a risk assessment to determine their IT assets’ value and the risk to those assets (see Figure 6-2). We find this figure surprisingly low. Canadian institutions were more likely to have undertaken risk assessments (48 percent), followed by doctoral institutions (39 percent). Note, however, that 51 percent of institutions with a dedicated IT security staff have undertaken a risk assessment. These are most often doctoral-extensive institutions (see Figure 6-3).

<table>
<thead>
<tr>
<th>Carnegie Class</th>
<th>Comprehensive Plan in Place</th>
<th>Partial Plan in Place</th>
<th>Currently Developing Plan</th>
<th>No Plan in Place</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Ext.</td>
<td>14.3</td>
<td>50.6</td>
<td>31.2</td>
<td>3.9</td>
<td>100.0</td>
</tr>
<tr>
<td>Dr. Int.</td>
<td>11.4</td>
<td>54.3</td>
<td>31.4</td>
<td>2.9</td>
<td>100.0</td>
</tr>
<tr>
<td>MA</td>
<td>9.9</td>
<td>45.0</td>
<td>34.2</td>
<td>10.8</td>
<td>99.9</td>
</tr>
<tr>
<td>BA</td>
<td>15.1</td>
<td>34.9</td>
<td>33.7</td>
<td>16.3</td>
<td>100.0</td>
</tr>
<tr>
<td>AA</td>
<td>13.7</td>
<td>31.4</td>
<td>47.1</td>
<td>7.8</td>
<td>100.0</td>
</tr>
<tr>
<td>Specialized</td>
<td>12.5</td>
<td>35.7</td>
<td>37.5</td>
<td>14.3</td>
<td>100.0</td>
</tr>
<tr>
<td>System</td>
<td>10.5</td>
<td>42.1</td>
<td>47.4</td>
<td>0.0</td>
<td>100.0</td>
</tr>
<tr>
<td>Total</td>
<td>12.6</td>
<td>41.8</td>
<td>35.9</td>
<td>9.7</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Figure 6-2. Has an IT Security Risk Assessment Been Undertaken?

Figure 6-3. Risk Assessment Undertaken, by Carnegie Class
We queried the periodicity of audits and vulnerability assessments and found that 9 percent perform IT security assessments monthly, 10 percent quarterly, and 26 percent annually. The rest responded “not regularly,” “never,” or “don’t know.” Again, doctoral-extensive institutions audited most often, usually on a monthly basis.

Also, we asked how often key enterprise systems and router configurations were audited to assess integrity and to look for unauthorized changes (see Figure 6-4). Forty-six percent audited on an irregular basis or not at all. Only 15 percent audited enterprise systems daily. These numbers appear to be surprisingly low, which suggests higher education has some work to do in the auditing area.

When we asked who conducted the reviews, 40 percent replied that an internal auditor conducted reviews; 55 percent used an external auditor, 22 percent used a vendor, and 35 percent used an external consultant. There was little difference by Carnegie class, size, country, and public versus private status in the use of vendors and external consultants. But doctoral and public institutions were by far most likely to use internal auditors and were also the largest employers of external auditors for this purpose.

Twenty percent of the institutions indicated that they had a risk assessment methodology for IT security. Only 12 percent of the institutions provided a guide or protocol for departments to conduct a self-assessment. Doctoral institutions were most likely to make a protocol available to departments, colleges, and business units.¹

### Updating and Maintaining Systems

When asked whether their implementation protocol required all new enterprise systems and applications to be tested or certified for IT security, 48 percent of respondents said their institution required testing and 20 percent required certification. Public

**Figure 6-4.** Audit Frequencies for Key Enterprise Systems and Router Configurations

<table>
<thead>
<tr>
<th>Audit Frequency</th>
<th>Percentage of Institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>14.9%</td>
</tr>
<tr>
<td>Weekly</td>
<td>8.5%</td>
</tr>
<tr>
<td>Monthly</td>
<td>7.4%</td>
</tr>
<tr>
<td>Quarterly</td>
<td>4.1%</td>
</tr>
<tr>
<td>Annually</td>
<td>6.0%</td>
</tr>
<tr>
<td>Not Regularly</td>
<td>39.1%</td>
</tr>
<tr>
<td>Never</td>
<td>40.0%</td>
</tr>
</tbody>
</table>

**Legend:**
- Red: Enterprise Systems
- Gray: Routers
institutions (60 percent) required testing and certification more than private institutions (40 percent).

It is important not only to update and maintain existing systems but also to build in appropriate security from the beginning. Jeffrey Savoy, information security officer at the University of Wisconsin–Madison, reflected on the importance of security being a part of system implementation. “We work to integrate security at the time systems are designed, developed, and implemented. It is critical. We bring the needed security expertise to the table. By involving security experts early in the system’s life, we can implement good security from the hardware up and can look at integration requirements from the beginning. Also, by seeking input from security experts early, a more accurate delivery date of the secure system can be obtained.”

Embry-Riddle Aeronautical University emphasized the importance of certification of their servers. According to Howard Muffler, chief security officer, “We certify our servers from the beginning—installed and prepared for whatever future action they are going to perform. They are certified along the way. They are also recertified from time to time, although that is not a policy or procedure. We ensure that over time the system does not degrade as we upgrade applications and operating systems.”

The EDUCAUSE 2002 Core Data Service (CDS) survey asked institutions whether all critical systems were expeditiously patched or updated, and 82 percent of the 621 institutions surveyed indicated that they were. Figure 6-5 shows the findings by Carnegie class.

The ECAR survey asked a similar question: how many critical systems and applications are required to be patched or updated in an expeditious manner? Fifty-three percent said that all of their systems had such a requirement, 32 percent said most, 11 percent said some, and 1 percent said none. There was no variation among institutions by size, Carnegie class, public versus private status, or country. These data appear to corroborate the 2002 EDUCAUSE CDS survey findings.

Most respondents (62 percent) agreed or strongly agreed that they required all campus-owned computers connected to the network to have known security holes fixed. Fifty-nine percent agreed or strongly agreed that their institutions conducted regular and frequent scans to detect known

Figure 6-5. Respondents Indicating that Critical Systems Are Expeditiously Patched or Updated, by Carnegie Class
security exposures in critical systems. But only 40 percent agreed or strongly agreed that their institution conducted regular and frequent scans to detect known security exposures in all campus computers connected to the network.

We compared the means for the above three requirements and viewed differences by Carnegie class (see Table 6-2). The scale used was 1 to 5, with one being strongly agree and 5 being strongly disagree. We found little difference among Carnegie class institutions with respect to both scanning questions, but we did see a negative progression from doctoral institutions (mean of 2.88) to associate’s institutions (mean of 1.98) with respect to mandating that holes be fixed on institution-owned computers, perhaps indicating a lessened ability to mandate IT security behavior. This may well be because of the diversity and complexity of undertaking such a task at research universities. However, the proliferation of self-replicating worms like Blaster and SQL

Table 6-2. IT Security Practices

<table>
<thead>
<tr>
<th>Carnegie Class</th>
<th>Require All Campus-Owned Computers Connected to Network to Have Known Security Holes Fixed</th>
<th>Conduct Regular and Frequent Scans to Detect Known Security Exposures in Critical Systems</th>
<th>Conduct Regular and Frequent Scans to Detect Known Security Exposures in All Campus-Owned Computers Connected to Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Ext. Mean</td>
<td>2.88</td>
<td>2.51</td>
<td>2.92</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.214</td>
<td>1.188</td>
<td>1.121</td>
</tr>
<tr>
<td>Dr. Int. Mean</td>
<td>2.40</td>
<td>2.23</td>
<td>2.79</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.288</td>
<td>1.239</td>
<td>1.274</td>
</tr>
<tr>
<td>MA Mean</td>
<td>2.34</td>
<td>2.47</td>
<td>3.07</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.181</td>
<td>1.106</td>
<td>1.139</td>
</tr>
<tr>
<td>BA Mean</td>
<td>2.32</td>
<td>2.52</td>
<td>2.95</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.104</td>
<td>1.087</td>
<td>1.221</td>
</tr>
<tr>
<td>AA Mean</td>
<td>1.98</td>
<td>2.18</td>
<td>2.67</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.010</td>
<td>1.014</td>
<td>1.088</td>
</tr>
<tr>
<td>Specialized Mean</td>
<td>2.28</td>
<td>2.73</td>
<td>3.02</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.140</td>
<td>1.326</td>
<td>1.269</td>
</tr>
<tr>
<td>System Mean</td>
<td>2.26</td>
<td>2.58</td>
<td>3.05</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.195</td>
<td>1.427</td>
<td>1.224</td>
</tr>
<tr>
<td>Total Mean</td>
<td>2.38</td>
<td>2.47</td>
<td>2.95</td>
</tr>
<tr>
<td>Std. deviation</td>
<td>1.179</td>
<td>1.166</td>
<td>1.177</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)
Slammer may change all of this because such automated attacks do not focus only on large, well known targets.

**Limiting and Controlling Access**

In Chapter 4 we discussed access control procedures and processes performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and limit access to a system’s resources to only authorized persons, programs, processes, or other systems. We noted also that traditional, multiple-use passwords predominate.

**Changing Passwords**

We asked institutions how often passwords were required to be changed (see Figure 6-6). Most respondents said 90 days or less (57 percent); 17 percent had no requirement. One baccalaureate institution required passwords to be changed daily. Table 6-3 shows common practice by Carnegie class.

![Figure 6-6. Password Change Frequency](image)

**Table 6-3. Password Change Frequency for Key Enterprise Systems, by Carnegie Class**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Carnegie Class (Percentage of Respondents)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dr. Ext.</td>
</tr>
<tr>
<td>Every 30 days</td>
<td>7.9</td>
</tr>
<tr>
<td>Every 60 days</td>
<td>11.8</td>
</tr>
<tr>
<td>Every 90 days</td>
<td>17.1</td>
</tr>
<tr>
<td>More than 90 days</td>
<td>38.2</td>
</tr>
<tr>
<td>No requirement</td>
<td>21.1</td>
</tr>
<tr>
<td>Don’t know</td>
<td>3.9</td>
</tr>
</tbody>
</table>
Eighty-eight percent felt that their procedures for identifying users before resetting passwords, tokens, and PINs were effective. Eighty percent of the institutions provide individuals with only enough access to do their jobs. There were no significant differences found among Carnegie classes or by institution size, public or private status, or country.

**Terminating Access**

Institutions for the most part are good at terminating access when users leave the institution (see Table 6-4). All said that they routinely terminate access to enterprise systems. Some, like the University of Minnesota, Twin Cities, give students an e-mail address for life. The institution doesn’t view termination as an end to all services and doesn’t believe e-mail access to be as important a security risk as other types of access.

**Background Investigations**

We asked whether employees and contractors with key access to enterprise systems had undergone criminal background investigation and whether they were bonded. These are not commonly used practices in higher education—indeed, 67 percent did not investigate for criminal background of employees and 95 percent did not bond them. Eighty-five percent did not require criminal investigation of contractors, and 71 percent said “no” to bonding. There were no significant differences found by Carnegie class, size of institution, public or private status, or country.

### Table 6-4. Access Termination

<table>
<thead>
<tr>
<th>Processes and Practices</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routinely terminate access to enterprise systems when users leave institution</td>
<td>100.0</td>
</tr>
<tr>
<td>Routinely terminate remote access when users leave institution</td>
<td>97.2</td>
</tr>
<tr>
<td>Routinely terminate e-mail access when users leave institution</td>
<td>96.4</td>
</tr>
<tr>
<td>Routinely terminate network access when users leave institution</td>
<td>94.1</td>
</tr>
<tr>
<td>Routinely terminate all access when users leave institution</td>
<td>90.7</td>
</tr>
<tr>
<td>Institution has procedure for identifying users before resetting passwords/tokens/PINs</td>
<td>84.9</td>
</tr>
</tbody>
</table>
Detection and Monitoring

According to the University of Washington's Terry Gray, the full spectrum of security embraces prevention, detection, and recovery. So far our focus has been on prevention. We now turn to detection and monitoring.

Monitoring User Accounts

We asked how often respondents’ institutions audited user account activity to detect dormant, invalid, or misused accounts as well as to audit access control lists (see Figure 6-7). With the exception of access control lists, which doctoral-extensive institutions were most likely to audit daily, we found no significant differences by Carnegie class, size of institution, public or private status, or country.

Monitoring Networks, Operating and Enterprise Systems, and Routers

Monitoring unusual activity on the network is key to preventing problems. Terry Gray sees proactive vulnerability probing as one of the most important tools available to secure a population of computers. It can be done centrally or by individual departments. Like most aspects of security, it is not a one-time activity but requires an ongoing and recurring effort.

Our data show that two-thirds of respondents monitor their networks daily (see Figure 6-8). When combined with weekly monitoring, the cumulative percentage rises to 80 percent. Operating systems are monitored slightly less frequently. It is not surprising that network monitoring is somewhat more prevalent, as commercial tools to

![Figure 6-7. Audit Frequency to Detect Dormant, Invalid, or Misused Accounts and Access Control Lists](image-url)
perform this task have been on the market for some time and are likely in use by many institutions’ network operations groups. On the other hand, tools to monitor for operating system or application vulnerabilities are newer on the scene and may not yet be as commonplace in many institutions.

Most institutions monitor their networks, operating systems, and enterprise systems daily. Larger institutions (in terms of student enrollments) and doctoral institutions are more likely to monitor on a daily basis. Overall, Canadian institutions monitor their networks more frequently than do U.S. institutions.

Terry Gray considers traffic-level monitoring a more promising strategy than pervasive intrusion detection. He believes institutions need to implement tools that monitor network traffic levels and send alerts when baseline thresholds are exceeded. With respect to intrusion detection, he said, “As network capacity and usage continue to escalate, it becomes increasingly difficult to believe that watching all network traffic for alarming patterns will prove to be a viable long-term solution. However, it may be reasonable to do for specific servers and can provide a validity check of whatever firewall rules may be in place.”

Endnote
In this chapter we address programs and practices that colleges and universities have implemented to respond to information technology (IT) security incidents. How do they identify and respond to incidents? Are some institutions more vulnerable than others, and if so, why? How does the institution respond to breaches and incidents? What is the impact on the institution?

The combination of university systems’ open nature and the high-powered technology that often exists on campuses puts academic institutions in a position unique among large enterprises. In addition to being the target of cyber attacks, university networks and systems sometimes serve as the source of attacks on other entities. For many institutions, being a good “Net citizen” and preventing the use of institutional resources for such attacks is nearly as high a priority as protecting their own information.

Examples of security breaches abound in higher education, and each one exposes the industry’s vulnerabilities, threats, and risks. A breach is as likely to come from within as outside the institution. Cornell University graduate student Robert Tappan Morris launched one of the first worms—the Morris Worm—in 1988. It was touted as the first worm that demonstrated the power of a self-replicating computer program across the network. The problems it caused led to the creation of the Computer Emergency Response Team (CERT) at Carnegie Mellon University, and this team remains a top organization for identifying viruses and notifying organizations and the general public about the effects of viruses and how to prevent their spread. (See the sidebar “Notable Viruses” for details about several of the most damaging viruses.) CERT also identifies security vulnerabilities, including viruses, and notifies organizations and the public about their effects and how to mitigate their exposure.

Cyber attacks are occurring with increasing frequency. A summer 2003 worm, referred to as the Microsoft remote protocol control incident, or “Blaster,” hit computer users with enormous speed. Unlike many worms, Blaster did not spread via e-mail but instead scanned the Internet looking for vulnerable computers. Symantec, maker of a leading antivirus software package, gave the worm a Category 4 threat-level rating on a scale of 5. The worm hit several universities hard. The University of Texas at Austin, for

Bandwidth spikes are rarely a result of academic breakthroughs.
—Dan Updegrove
Notable Viruses

The Love Bug (I Love You) virus is one of the best-known viruses worldwide. This virus only targeted users running the Microsoft Windows operating system, attacking the Outlook e-mail program and the Internet Explorer browser. When opened, the virus attacked the computer’s hard drive, deleting video and digital photography files and hiding music files. The file forwarded itself to all addresses in the Microsoft Outlook address book. The virus may have erased files from its victims’ computers, but the more widespread damage was in clogging up computer networks. This virus was one of the most destructive ever developed, with effects ranging from corrupted data files to the wholesale destruction of a company’s data records. Estimates of the damage caused range up to $10 billion, mostly in lost work time.

The Melissa Virus, a widespread virus in 1999, infected more than a million computers. The virus affected only computers with Microsoft operating systems, attacking the Microsoft Outlook program to propagate itself. When a user opened the infected e-mail attachment, the virus attempted to e-mail a copy of this document to up to 50 other people. This was significant to many users, as it had the potential to compromise organizational confidentiality. While the virus did comparatively little damage to individual computers, unlike later viruses, it had graver implications for company and Web servers carrying the huge volumes of e-mail being created. The virus, believed to have been named after a Florida stripper its creator knew, caused more than $80 million in damage.

The Code Red Worm first appeared in July 2001. Originally designed as a denial-of-service attack on the White House Web site, it had the power to infect 250,000 systems in just nine hours. The self-spreading program infected servers using unpatched versions of Microsoft’s Internet Information Server software and defacing the Web sites the servers hosted. The worm spread by selecting one hundred IP addresses, scanning the computers associated with them for a hole, and spreading to the vulnerable machines. It then defaced any Web site hosted by the server. The worm could also help attackers identify infected computers and gain control of them. The effects of Code Red were devastating and widespread. It is estimated that Code Red infected more than one million of the 5.9 million Microsoft IIS Web servers. Additionally, many companies experienced internal disasters when 25 or more system infections simultaneously occurred. While the main effects were performance degradation and system instability, the Code Red worm also caused billions of dollars in damage and introduced the technol-
ogy community to the dangers of not reacting quickly to public warnings of vulnerabilities.

Called a “multiexploit” worm, Nimda used several methods to spread around the world, including e-mail and unpatched IIS servers. In 2001, Nimda was the first worm to modify existing Web sites to start offering infected files for download. It was also the first worm to use normal end-user machines to scan for vulnerable Web sites. This technique enabled Nimda to easily reach intranet Web sites located behind firewalls—something other worms couldn’t directly do. This complex virus contained a mass-mailing worm component that spread itself to Windows users in attachments named README.EXE and then quickly spread around the world. The worm created network outages worldwide, and the extent of the damage appeared throughout the Internet, causing very poor Internet connectivity, damaged Web sites, and an inability to connect to various host servers, mail servers, and Web sites. The immense volume of traffic generated by the virus either brought down network routers around the world or slowed them to a halt.

Chernobyl was the first virus to damage computer hardware. The virus struck on 26 April 1999, the anniversary of the Chernobyl nuclear disaster, and affected computers running Windows 95 and 98, striking them as they were booted up. The virus rendered hard drives unusable and, in some cases, damaged the hardware that allows computers to start up. Hundreds of thousands of computers in Asia and the Middle East had their data wiped by the Chernobyl virus, but the United States and Europe managed to escape most of its harmful effects. Estimates of damage reached into the hundreds of millions of dollars.

Happy99 has been called the first modern Internet worm discovered “in the wild.” The worm was distributed in early January 1999 as a Windows .exe file attached to an e-mail message. When run, it displayed fireworks on the screen. At the same time, it changed the machine’s network software so that every time an e-mail was sent from the machine, a copy of Happy99 was also sent to the same address. There was no other malicious payload apart from its system modifications to facilitate its propagation.

In February 2000, widespread denial-of-service attacks made headlines as they crippled the online operations of Amazon.com, Yahoo, eBay, CNN, and Buy.com. These Web sites were flooded with thousands of bogus messages, making it difficult or impossible for genuine users to connect to the site. Many of these prominent Web sites suffered major slowdowns, with some having to shut down for several hours until they could restore service.
example, scanned their network and found 5,000 machines infected. They blocked IP addresses at the border and as close to the switch as possible. They then sent a message to owners requesting that they install the patch; two days later they sent a more emphatic message, resulting in significant user community compliance.

Institutions that avoided problems had one or more of the following factors in place:

- a significant Macintosh presence on campus;
- implementation of port blocking, including permanent blocking of ports (NetBIOS protocol), or ad hoc blocking in response to notification from FIRST (Forum of Incident Response Teams) and subsequent announcements from the Department of Homeland Security and REN-ISAC;
- availability of virtual private network (VPN) service as an alternative; and
- proactive scanning and effective intrusion detection, allowing for early detection of the problem.

Border blocks plus VPNs appeared to be the most effective and desirable practice for minimizing this worm’s impact on end users.

On 5 June 2003, confidential employee salary and bonus information was transmitted on the Web to some of the 35,000 computer users inside Stanford University when the Bugbear.B virus that infected the university’s computer system randomly sent out files from campus PCs. Chris Handley, CIO at Stanford University, responded by temporarily blocking users from sending e-mail to the outside world.

In February 2003, a computer hacker obtained the names and Social Security numbers of about 59,000 former and current students, faculty, and staff members at The University of Texas at Austin. Dan Updegrove, CIO, estimated that this cost the institution $145,000 to $150,000, including $25,000 to print and mail letters, $2,000 in phone bills and third-party payments for address cleanup, and $100,000 in staff time.

In January 2003, University of Kansas officials detected suspected computer hacking into a file server that contained records of 1,450 students, mostly international students. In June 2002, the Chronicle of Higher Education reported the possibility that Russian mafia had infiltrated computers at Arizona State and other colleges.

Another and more recent insidious form of intrusion comes from so-called spyware—software that gets installed surreptitiously via browser hijackers, adware, auto dialers, and some freeware applications. When a user clicks on a pop-up ad, spyware resets the browser home page and inserts bookmarks that are difficult to delete. Typically, they will redirect the user to porn and gambling sites. Such attacks impede work, which is costly to the institution.

The University of Washington’s Terry Gray classifies these threats to higher education institutions in seven categories:

- application-level security threats such as e-mail viruses, attachments, and IRC bots;
- threats to network infrastructure devices (switches, routers);
- threats to core network computing services (DNS, DHCP, Kerberos);
- theft of network connectivity services by unauthorized users;
- unauthorized access to hosts (both clients and servers) via the Internet;
- unintended disclosure or modification of data sent between hosts; and
- denial-of-service attacks against connected hosts.

Each has been a reality for higher education. KPMG Consulting LLC provided the University of California with a useful analysis of hacker attack profiles.² It outlined 10 of the
of-service attack, and 12 percent Web site intrusion (hacking).

These attacks rack up substantial costs. According to findings from the 2003 CSI/FBI Computer Crime and Security Survey, theft of proprietary information from businesses caused the greatest financial loss, with the average reported loss being approximately $2.7 million. The second most expensive computer crime among survey respondents was denial of service, followed by financial fraud. Virus incidents (82 percent) and insider abuse of network access (80 percent) were the most often cited forms of attack or abuse.

**IT Security Incidents**

Eighty institutions (19 percent of respondents) indicated that they had an IT security incident that had been reported to the press. The larger institutions and doctoral institutions were more likely to have had such an incident (see Figures 7-1 and 7-2). Of the 19 institutions with enrollments of more than 25,000 in our study, 58 percent had an in-

---

**Figure 7-1. IT Security Incident Reported in the Press, by Student Enrollment**

- **Up to 2,000**: 5.1%
- **2,001–4,000**: 6.9%
- **4,001–8,000**: 15.2%
- **8,001–15,000**: 37.1%
- **15,001–25,000**: 39.2%
- **More than 25,000**: 57.9%
incident reported in the press, compared with 5 percent at institutions with enrollments of 2,000 or fewer.

Of course, this does not mean that others are exempt. Of the total incidents reported in the press, 30 percent were at institutions with 8,000 or fewer enrolled students, 30 percent at institutions with enrollments between 8,001 and 15,000, 25 percent at institutions with enrollments between 15,001 and 25,000, and 15 percent at institutions with enrollments of more than 25,000.

Doctoral-extensive institutions (51 percent), followed by doctoral-intensive institutions (29 percent) and MA institutions (13 percent), had the most incidents reported in the press. And these institutions were attacked more often. Note also that 70 percent of the reported incidents occurred at public institutions, which may reflect more stringent public reporting requirements.

We also asked when the respondents’ institutions experienced their first incident that was reported to the press. Only 71 of the 435 institutions gave us the year or period. Of that subgroup, 63 percent indicated after 2000, 28 percent during 1997–1999, and 1 percent before 1996. We found little difference by Carnegie class, size, public versus private status, or country.

**Residence Halls and Incidents**

Residence halls connected to the campus network are often cited as a large area of potential risk because they provide a less controlled computing environment. Consequently, they raise a potential IT security threat from within the institution and also expose the campus network to the possibility of attack on unsecured machines. According to Diana Oblinger, executive director of
higher education at Microsoft and former ECAR senior fellow, “Students are able to bring their own computer equipment and connect to the network. The software on those computers can be from a host of vendors representing an array of versions, and both students and vendors might be unaware of security problems in those products. The transient nature of the student population creates additional security challenges, while the advent of wireless capabilities generates further problems.”

Do residence halls make a difference? Have institutions with residence halls deployed different strategies than those without residence halls? Of the institutions surveyed, 76 percent had residence halls (67 percent in Canada). Those with residence halls were more likely than those without to have policies for shutting off Internet access (89 percent versus 68 percent) and formal incident handling procedures (48 percent versus 34 percent). However, we found little difference in enforcement procedures and willingness for administrators to take punishable action in general. While student awareness programs were more likely at institutions with residence halls (37 percent versus 22.5 percent), these percentages seem low, given the potential exposure. Moreover, the respondents did not rate their programs’ effectiveness differently. Finally, institutions with residence halls were more likely to have a security incident reported in the press (22 percent versus 8 percent). Residence-hall computing increasingly is managed differently, with many institutions setting up separate networks for them.

**IT Security Incident Handling Procedures**

We asked respondents whether their institution had a formal IT security incident handling procedure. Forty-five percent said they did (43 percent in Canada), compared with 66 percent of KPMG survey respondents. Institutions most likely to have formal incident procedures are public, doctoral, and those with more than 25,000 students enrolled.
Figure 7-4 shows the breakdown by Carnegie class, Figure 7-5 by student enrollment, and Figure 7-6 by number of networked devices. Clearly, as enrollments increase, so does the likelihood of having a formal procedure. Without one, many organizations cannot accurately assess damage done to the institution or effectively handle internal and external public relations.

Our interviews revealed that several institutions had “incident policies” used for any incident—not just IT security ones. Typically, the press office or the Office of University Affairs handles the press, bringing in other officials—IT officers, senior management—as appropriate. The University of Notre Dame, which did have an incident reported in the local press, has a specific policy for IT security. CIO Gordon Wishon said, “We have a director of communications that coordinates with the rest of the campus. Our process involves any one or a mix of people, depending upon the nature of the incident; it depends upon the vector. If it is an incident that is reported through the police department/public safety, I may not be involved in the front end of the process. If it is an incident that we become aware of internally, it would rise to me very quickly, and yes, we would involve the appropriate people along the way.”

According to Dick Jacobson, North Dakota University System IT security officer, “In larger institutions, departments may handle an incident response, too, since their IT security operations are decentralized. Our policy gives the individual campus the responsibility to deal with the incident. Realistically, however, we tend to find out or get involved pretty early in the process, and we have expertise that can be leveraged by the smaller institutions.”

The Georgia Institute of Technology (Georgia Tech) has a highly formalized incident response team and policies. The procedures are documented in a flowchart, which contains contact information and illustrates specific actions resulting from incident...
Figure 7-5. Institutions with Formal Procedures for Handling IT Security Incidents, by Student Enrollment

Figure 7-6 Institutions with Formal Procedures for Handling IT Security Incidents, by Number of Networked Devices
events. John Mullin, associate vice provost, associate vice president, and chief information officer for information technology, said, “Incident response policies are tools to help you deal with the incident more effectively and more quickly. We weren’t paralyzed when the incident occurred. After you get past the expletives, you have a process to follow. We tune it for the next round, and we hope we never need it—just like insurance.”

At the University of Wisconsin–Madison, volunteers participate on the BadgIRT (Badger Incident Response Team), which operates as an integral part of the Division of Information Technology’s security department. It acts as a central collection point for tracking incidents, analyzes information security trends, and works with other incident response teams worldwide. BadgIRT is a member of FIRST. “BadgIRT is very important to security efforts at UW–Madison,” emphasized Judy Caruso, director of policy, security, and planning. “As a very decentralized campus, it is imperative to have active involvement and engagement in security incidents and directions by IT staff from throughout the campus.”

Who Is Involved in IT Security Incident Handling Procedures?

We asked for further elaboration on who gets involved if an incident occurs. In descending order, 86 percent of the procedures included the police and campus security offices, 75 percent the student judicial affairs office, 74 percent the legal office (general counsel), and 65 percent the campus communications office. Among institutions that had formal procedures, we found little difference by size, Carnegie class, public or private status, or country. There was a significant difference, however, by size and Carnegie class with respect to involving the police and legal counsel. Doctoral institutions (90 percent) and institutions with more than 25,000 enrolled students (100 percent) were far more likely than the smallest institutions (60 percent) to include the police and legal counsel.

Georgia Tech created an executive response team for incident response consisting of the CIO, the director of auditing, the director of information security, the director of financial services, the vice president of human resources, the director of campus communications, the legal counsel, and the director of campus security. In addition, the head of the affected unit joins the team for the duration of the response.

The University of Texas at Austin’s central information security office has formal interfaces to the rest of the campus community: legal affairs, public affairs, the University of Texas system office general counsel, the University of Texas police department, and the district attorney’s office. According to Dan Updegrove, vice president for information technology at The University of Texas at Austin, “When you are in the middle of a high-profile security breach, you’d better have a really good partnership among public affairs, legal affairs, the president’s office, and IT. It served us enormously well to have a very sophisticated public affairs office that had good relations with the press and a legal affairs office that understands information technology. They quickly grasped the problem and its many dimensions. We all worked together to create a systematic response.”

We also asked whether the formal procedures included central mechanisms for alerting faculty, staff, students, and the administration. Eighty-three percent of respondents answered “yes.” Among institutions that had formal procedures, we found little difference by size, Carnegie class, public or private status, or country.
Reporting Incidents to Senior Management

Asked when they report incidents to senior management, 71 percent of respondents indicated the choice “when the incident occurs.” Combined with the answer “not regularly,” the total becomes 86 percent. Only 14 percent regularly report incidents to senior management. We investigated whether institutions that are attacked most often and were among the first institutions attacked had different reporting patterns than those that were attacked less often or did not have incidents reported in the press. The numbers were so low that we couldn’t come to a conclusion. The case studies and in-depth interview data provide a better perspective.

Recent attacks and security breaches at Indiana University provided a catalyst for improving that university’s security and incident response, including adoption of a formal incident response methodology. Using a central incident response reporting system, central security staff log incidents and triage them. If they suspect a compromise, they identify the incident's location and the system administrator for that location and ask the system administrator to respond immediately. If the system administrator doesn’t respond, central staff have the ability to isolate the machine from the network. “This is rare, though,” noted Merri Beth Lavagnino, deputy policy officer. “Maybe 5 to 10 percent of the time we don’t have records identifying the appropriate system administrator.”

Both Florida Memorial and Notre Dame report that their incidents accelerated their IT security efforts. For example, Notre Dame’s Gordon Wishon stated that after the local press reported the intrusion into a system containing Social Security numbers of hourly wage earners, “it showed that our rollout or deployment of security provisions and best-practice implementation within the OIT and within the data center was not proceeding with enough haste, and it resulted in a substantial [acceleration] of the security program, including the erection of barriers around the data center.”

EDUCAUSE Quarterly reported an interesting case study of the ramifications of a security incident at the University of Memphis. Written by Robert Jackson, systems administrator in the information technology division at the University of Memphis, and Mark N. Frolick, Western and Southern Financial Chair in information systems at Xavier University in Cincinnati, Ohio, the article elaborated on personnel roles in the case of a security breach, detection and forensics, and policy enforcement. It also enumerated lessons learned and offered important, broadly applicable recommendations to mitigate security exposure.

IT security incidents continue to increase and are a problem industry-wide. In the next chapter, we address more directly what institutions must do to protect themselves from IT security incidents.

Endnotes
1. There is an ongoing debate about the meaning of open networks.
2. “Net Security,” topic paper for the University of California, prepared by KPMG Consulting LLC, no date.
In this chapter we describe the perceived level of success information technology (IT) security programs have attained at our institutions and discuss factors that contribute positively and negatively to their success. Included are technologies in use, staff experience, institutional size, the organization of campus IT security, the presence of policies and IT security plans, awareness programs, and budget.

How Successful Are We?

We used a Likert scale ranging from 1 to 5 (1 is strongly agree, 2 is agree, 3 is neutral, 4 is disagree, and 5 is strongly disagree) to assess each respondent's opinion on the success of his or her institution's IT security programs and on benchmarks for success. We asked five questions:

- How would you characterize your program's success?
- Has your institution gone beyond federal and state government IT security requirements?
- Are data, networks, and applications that are your responsibility secure?
- Have you developed metrics to determine IT security activities' effectiveness?
- Is your institution more secure today than it was two years ago?

We calculated the mean for each question and then compared the means by Carnegie class, along with a category for Canadian institutions (see Table 8-1).

The respondents were most positive about feeling more secure today than two years ago despite being in what we perceive as a riskier environment. The mean of 1.86 shows that a majority agreed or strongly agreed that their institutions were more secure today. The next most positive response was to the question, "How would you characterize the success of your IT security program?," with a mean for all of 2.40. We found little difference on any of the questions by Carnegie class, number of devices and users, or country.

What our respondents appear to be telling us is that they feel more secure today, but their IT security programs still need strengthening. Interestingly, when we asked respondents individually about the data, networks, and applications they were responsible for, the answers were less positive, though still positive overall. Most respondents felt that they had not gone beyond state and federal requirements, nor

Security is a negative deliverable. You don’t know when you have it. You only know when you’ve lost it.
—Jeffrey I. Schiller

© 2003 EDUCAUSE. Reproduction by permission only.
had they developed metrics to determine their IT security programs’ effectiveness. So, for the most part, assessing the security level remains, for many institutions in our survey, a subjective exercise.

The people we interviewed had varying opinions about what constituted success. Bruce Judd, associate vice president at San Jose State University, stated, “Success is measured by the number of problems we have. When I look at the number of problems we had a year ago and the number of problems we have today, the reduction is dramatic. I feel that we have been successful in reducing the number of incidents, but it is not as successful as we could be and where we need to go—to the point where we stabilize the network, reduce the incidents and their severity down to a minimum, and where they are no longer visible to the campus.”

Dick Jacobson, North Dakota State University System IT security officer, attributed his institution’s success in part to organizational changes. “I think our program is effective, and the effectiveness has grown because of the formalized structure that we have put in place with designated security officers on the campuses. There is a defined flow of communication.”

Morrow Long, information security director at Yale University, measured success by incrementally improving IT security programs. “IT security at Yale University is effective: over time we have been able to achieve quite a bit in terms of increasing security—moving the university off insecure protocols and implementing internal firewalls, authentication systems, standards, policies, and procedures for securing machines. It is an incremental, evolutionary approach, year by year—but we have moved quite a bit in terms of where we were.”

Paul Howell, information systems security officer at the University of Michigan, is more cautious about success. “It is hard to judge

<table>
<thead>
<tr>
<th>Carnegie Class</th>
<th>Program Is Successful</th>
<th>Beyond Requirements</th>
<th>Systems Are Secure</th>
<th>Metrics Developed</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Ext.</td>
<td>2.32</td>
<td>3.27</td>
<td>2.78</td>
<td>3.42</td>
<td>1.78</td>
</tr>
<tr>
<td>Dr. Int.</td>
<td>2.35</td>
<td>3.21</td>
<td>2.74</td>
<td>3.44</td>
<td>1.83</td>
</tr>
<tr>
<td>MA</td>
<td>2.31</td>
<td>3.49</td>
<td>2.79</td>
<td>3.68</td>
<td>1.95</td>
</tr>
<tr>
<td>BA</td>
<td>2.35</td>
<td>3.28</td>
<td>2.53</td>
<td>3.60</td>
<td>1.84</td>
</tr>
<tr>
<td>AA</td>
<td>2.27</td>
<td>2.98</td>
<td>2.46</td>
<td>3.28</td>
<td>1.77</td>
</tr>
<tr>
<td>Specialized</td>
<td>2.34</td>
<td>3.25</td>
<td>2.65</td>
<td>3.47</td>
<td>1.89</td>
</tr>
<tr>
<td>System</td>
<td>2.31</td>
<td>3.06</td>
<td>3.00</td>
<td>3.52</td>
<td>2.00</td>
</tr>
<tr>
<td>Canada</td>
<td>2.40</td>
<td>3.44</td>
<td>2.76</td>
<td>3.67</td>
<td>1.95</td>
</tr>
<tr>
<td>All Respondents</td>
<td>2.31</td>
<td>3.28</td>
<td>2.68</td>
<td>3.52</td>
<td>1.86</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)
success because we are really in the business of risk management. If nothing happens, does that mean we are successful? Or if there is a major, national-headline incident, does that mean we are unsuccessful?"

The absence of benchmarks—a problem for higher education in all business areas—makes it difficult to measure success.

**IT Security: What Matters**

Our data show that although using more sophisticated technologies has significantly enhanced IT security, institutions have placed even more importance on the human and cultural factors of campus life. They recognize that they must address “human frailty” for the higher education environment to be secure. Indeed, our data show that respondents perceive managing security to be at least as much of a people problem as a technology problem. In the following sections, we demonstrate that “soft” IT security interventions (organization, policies, awareness programs, executive attention) seem to make respondents feel more secure than do “hard” interventions such as technology investments.

**Organization Matters**

Table 8-2 compares opinions about success among institutions that have a dedicated IT security staff, a single staff member, and a distributed staff. It shows that institutions with a dedicated staff do markedly better in all five areas. We attribute this to the activities that dedicated security staff can and have undertaken and completed. A dedicated staff has the time to see that various IT security tasks are done, and in a more holistic manner. The presence of a dedicated staff (more prevalent at larger institutions) can denote a level of professionalism, which then drives practices and procedures implemented and technology deployed. The number of staff employed was less significant than having a dedicated staff. The staff’s experience also seemed to make a difference: institutions with staff who had more than three years

<table>
<thead>
<tr>
<th>Staffing Model</th>
<th>Program Is Successful</th>
<th>Beyond Requirements</th>
<th>Systems Are Secure</th>
<th>Metrics Developed</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single staff member</td>
<td>Mean 2.47</td>
<td>3.34</td>
<td>2.78</td>
<td>3.57</td>
<td>1.94</td>
</tr>
<tr>
<td>Dedicated security operations staff</td>
<td>Mean 2.00</td>
<td>2.98</td>
<td>2.49</td>
<td>3.06</td>
<td>1.56</td>
</tr>
<tr>
<td>Spread across multiple functions</td>
<td>Mean 2.28</td>
<td>3.31</td>
<td>2.67</td>
<td>3.59</td>
<td>1.89</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)
of experience felt they were doing better than those whose staff had three years or less of experience.

**IT Security Policies, Planning, and Formal Risk Assessments Matter**

In Chapter 5 we noted the adoption level of formal IT security policies and presented some of the reasons for putting policies in place. Our data (see Table 8-3) show that institutions with IT security policies in place characterize their IT security programs as more successful and feel more secure today. Michael McRobbie, vice president for information technology and CIO at Indiana University, advised, “Policy comes first; then security. You can get preoccupied with tactics and lose sight of the grand scheme. You need constant policy education. Put policies in place that make security possible.”

We also find an improved sense of security when IT security is part of an IT security plan (see Table 8-4). Note also that metrics are more likely to have been developed at

### Table 8-3. Success and Formal Institutional Policies

<table>
<thead>
<tr>
<th>Formal Institutional Policies</th>
<th>Program Is Successful</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Mean 2.110</td>
<td>1.760</td>
</tr>
<tr>
<td></td>
<td>Std. deviation 0.684</td>
<td>0.792</td>
</tr>
<tr>
<td>No</td>
<td>Mean 2.550</td>
<td>1.990</td>
</tr>
<tr>
<td></td>
<td>Std. deviation 0.777</td>
<td>0.864</td>
</tr>
<tr>
<td>Total</td>
<td>Mean 2.310</td>
<td>1.860</td>
</tr>
<tr>
<td></td>
<td>Std. deviation 0.759</td>
<td>0.833</td>
</tr>
</tbody>
</table>

*Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)*

### Table 8-4. IT Plan Characteristics and Perceived Success

<table>
<thead>
<tr>
<th>Security Part of IT Plan</th>
<th>Program Is Successful</th>
<th>Metrics Developed</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Mean 2.200</td>
<td>3.370</td>
<td>1.760</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation 0.753</td>
<td>0.892</td>
<td>0.796</td>
</tr>
<tr>
<td>No</td>
<td>Mean 2.540</td>
<td>3.870</td>
<td>2.180</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation 0.670</td>
<td>0.755</td>
<td>0.893</td>
</tr>
</tbody>
</table>

*Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)*
institutions that have an IT security plan and audit regularly.

Also, we find a similar improved sense of security when risk assessments have been completed (see Table 8-5).

**Leadership Matters**

We asked respondents whether their president and provost had been active in developing IT security policy (see Table 8-6). While the mean is lower than expected overall, we clearly see an impact when the president and provost are involved. At institutions where the president is involved, for example, the mean score for success is 3.18, compared with 4.50 at institutions where the president has not been involved (measured on a 5-point Likert scale, with 1 being highly successful and 5 being highly unsuccessful).

Clark Sorensen, manager of information systems and services and senior assistant registrar at Indiana University, emphasized the importance of leadership. “Since McRobbie came on campus, the campus

Table 8-5. Success and Risk Assessment Undertaken

<table>
<thead>
<tr>
<th>Risk Assessment Undertaken</th>
<th>Program Is Successful</th>
<th>Metrics Developed</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Mean 2.03</td>
<td>3.15</td>
<td>1.64</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation 0.745</td>
<td>0.892</td>
<td>0.684</td>
</tr>
<tr>
<td>No</td>
<td>Mean 2.44</td>
<td>3.71</td>
<td>1.97</td>
</tr>
<tr>
<td></td>
<td>Std. Deviation 0.742</td>
<td>0.829</td>
<td>0.851</td>
</tr>
</tbody>
</table>

*Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)*

Table 8-6. Impact of the President and Provost in Developing Policy

<table>
<thead>
<tr>
<th>Program Success</th>
<th>President Involved</th>
<th>Provost Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly successful</td>
<td>3.18</td>
<td>3.28</td>
</tr>
<tr>
<td>Fairly successful</td>
<td>3.64</td>
<td>3.35</td>
</tr>
<tr>
<td>Neither</td>
<td>3.86</td>
<td>3.69</td>
</tr>
<tr>
<td>Fairly unsuccessful</td>
<td>3.92</td>
<td>4.00</td>
</tr>
<tr>
<td>Highly unsuccessful</td>
<td>4.50</td>
<td>4.50</td>
</tr>
<tr>
<td>Total</td>
<td>3.67</td>
<td>3.47</td>
</tr>
</tbody>
</table>

*Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)*
culture regarding security has changed. We more stringently ensure that people don’t get to data that they shouldn’t have. People at Indiana University are taking IT security seriously.”

McRobbie advised, “Get your president on your side. Get him to say security is important publicly.” McRobbie immediately established a good working relationship with then-President Myles Brand, who became a strong advocate for IT security. Executive-level support enabled Indiana University to proceed more quickly in adopting good security practices than it could have without this support.

Size Matters

We looked at the size of institutions along three dimensions: enrolled students, number of devices on the network, and number of users on the network. We then tested to see if size mattered, and if so, where. As we demonstrate, size does matter. And most often, it is the number of devices on the network that seems to matter most.

Table 8-7 shows that as the number of network devices increases, the likelihood of having a dedicated IT security staff increases. As institutions grow to more than 5,000 devices, they begin to deploy a dedicated IT security staff. And as we noted earlier in this chapter, the presence of a dedicated IT security staff has a noticeable impact on IT security and behavior at institutions.

Similarly, we found a greater likelihood of having a formal policy (Figure 8-1) and a formal incident handling procedure among institutions with more than 5,000 networked devices.

As the number of devices increases, the issue of decentralization causes greater concern (Figure 8-2), as does the fear of an

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Single Staff Member</th>
<th>Dedicated IT Security Staff</th>
<th>Decentralized Security Staffing</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 1,000</td>
<td>29.4</td>
<td>0.0</td>
<td>50.0</td>
<td>20.6</td>
</tr>
<tr>
<td>1,001–5,000</td>
<td>26.4</td>
<td>2.6</td>
<td>59.6</td>
<td>11.4</td>
</tr>
<tr>
<td>5,001–10,000</td>
<td>24.3</td>
<td>18.9</td>
<td>51.4</td>
<td>5.4</td>
</tr>
<tr>
<td>10,001–20,000</td>
<td>4.3</td>
<td>27.7</td>
<td>66.0</td>
<td>2.0</td>
</tr>
<tr>
<td>20,001–40,000</td>
<td>0.0</td>
<td>30.4</td>
<td>65.2</td>
<td>4.4</td>
</tr>
<tr>
<td>40,001–60,000</td>
<td>8.3</td>
<td>41.7</td>
<td>50.0</td>
<td>0.0</td>
</tr>
<tr>
<td>More than 60,000</td>
<td>0.0</td>
<td>55.0</td>
<td>45.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>
Figure 8-1. Relationship Between IT Security Policies and Networked Devices

Figure 8-2. Decentralization Perceived as IT Security Barrier, by Number of Networked Devices
IT security problem occurring because of an authorized campus user’s inadvertent action (Table 8-8).

**Awareness Programs Matter**

Similarly, the presence of awareness programs increases the sense of security (see Table 8-9). Awareness programs and IT security go hand-in-hand.

**Money Matters**

Absence of resources was by far the largest barrier to IT security for our respondents. We asked five questions about the IT security budget: What percentage of the IT budget is spent on security? Does the institution provide sufficient funds for IT security? (The latter question used a 5-point Likert scale, with 1 being strongly agree and 5 being strongly disagree.) How does budget impact IT security? Do you feel better? Are purchases of technology affected?

Table 8-10 indicates the percentage of the central IT budget spent on security and compares respondents’ mean assessments of IT security program success and whether they feel more secure today than two years ago. It appears that the more you spend, the better you feel!

Similarly, respondents who believe their institution provides necessary resources give higher ratings for IT security program success and their current sense of IT security (Table 8-11). The data also show that institutions

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 1,000</td>
<td>2.88</td>
<td>0.937</td>
</tr>
<tr>
<td>1,001–5,000</td>
<td>2.71</td>
<td>1.105</td>
</tr>
<tr>
<td>5,001–10,000</td>
<td>2.51</td>
<td>1.010</td>
</tr>
<tr>
<td>10,001–20,000</td>
<td>2.34</td>
<td>0.891</td>
</tr>
<tr>
<td>20,001–40,000</td>
<td>2.17</td>
<td>0.834</td>
</tr>
<tr>
<td>40,001–60,000</td>
<td>2.33</td>
<td>0.651</td>
</tr>
<tr>
<td>More than 60,000</td>
<td>1.60</td>
<td>0.548</td>
</tr>
</tbody>
</table>

*Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)*

<table>
<thead>
<tr>
<th>Formal IT Security Awareness Program for Staff</th>
<th>Program Is Successful</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Mean 2.000</td>
<td>1.660</td>
</tr>
<tr>
<td></td>
<td>Std. deviation 0.592</td>
<td>0.661</td>
</tr>
<tr>
<td>No</td>
<td>Mean 2.500</td>
<td>1.980</td>
</tr>
<tr>
<td></td>
<td>Std. deviation 0.799</td>
<td>0.898</td>
</tr>
</tbody>
</table>

*Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)*
Table 8-10. Assessment of IT Security Program Success Compared with IT Budget

<table>
<thead>
<tr>
<th>Percentage of Central IT Budget for IT Security</th>
<th>Program Is Successful</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1</td>
<td>2.56</td>
<td>2.16</td>
</tr>
<tr>
<td>1–5</td>
<td>2.30</td>
<td>1.82</td>
</tr>
<tr>
<td>6–10</td>
<td>2.00</td>
<td>1.62</td>
</tr>
<tr>
<td>11–15</td>
<td>1.60</td>
<td>1.20</td>
</tr>
<tr>
<td>16–20</td>
<td>1.50</td>
<td>2.00</td>
</tr>
<tr>
<td>Over 20</td>
<td>1.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

Table 8-11. IT Security Program Success Compared with Resources Provided

<table>
<thead>
<tr>
<th>Institution Has Provided Needed Resources</th>
<th>Program Is Successful</th>
<th>More Secure than Two Years Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>1.30</td>
<td>1.20</td>
</tr>
<tr>
<td>Agree</td>
<td>1.92</td>
<td>1.65</td>
</tr>
<tr>
<td>Neutral</td>
<td>2.28</td>
<td>1.81</td>
</tr>
<tr>
<td>Disagree</td>
<td>2.50</td>
<td>1.97</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>2.96</td>
<td>2.28</td>
</tr>
<tr>
<td>Total</td>
<td>2.31</td>
<td>1.86</td>
</tr>
</tbody>
</table>

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)
that spend a higher percentage of the IT budget on security and provide sufficient resources have purchased more technology and invested more in awareness programs. Money matters!

**IT Security Barriers**

We have discussed at some length factors that contribute to IT security programs’ success. We turn now to barriers that hinder IT security.

We asked respondents to identify and assess barriers to IT security at their institutions (see Figure 8-3). By far the most common problem cited was lack of resources (72 percent), followed by lack of awareness (46 percent) and cultural reasons such as academic freedom (32 percent) and culture of decentralization. External factors such as laws and their timely implementation and clarification, technology, software, and hardware scored much lower. We were surprised by the lower scores given to vendor hardware and software and the legal environment.

We looked at Carnegie class to find any major differences of opinion by institution type and found little, with two exceptions. Not surprisingly, a culture of decentralization was primarily an issue at doctoral institutions. Baccalaureate institutions most often mentioned individual privacy, but the percentage was low in any event. President James Wright of Dartmouth College believes the complex interrelationship between security and privacy will emerge as the most controversial issue.¹

Respondents saw decentralization as a barrier at many complex institutions. At Indiana University, for example, respondents noted the natural tension and synergy between the centralized policy development and security programs and the decentralized units. According to Beth Cate, associate university counsel, “Tensions can arise because some units historically have operated their systems in a decentralized way and generally favor as much autonomy as possible in the services of academic freedom, but their technological expertise and resources may vary.

![Figure 8-3. Perceived Barriers to IT Security](image-url)
and create substantial risks to the security of those systems. The key in lessening this tension is good communication between the centralized IT offices and the units that emphasize the help that the central offices can provide the units in meeting their computing needs while ensuring an appropriate level of security for their systems, and that also educates the units about the risks involved with decentralization.”

Paul Howell, information systems security officer at the University of Michigan, provided a fairly typical assessment of institutional barriers. “Money and resources are always issues,” he said. “We have a lot of legacy equipment. The decentralized nature of the university from a security viewpoint is more of a hindrance than help. Sponsored research needs to be operated in a secure manner and is expected to do so by the federal government. But it does not appear that the federal government wants to provide funding for this purpose. We need a greater partnership between universities and the federal government and a reexamination of the infrastructure or overhead that exists around hosting research work.” Competent system administration time, security technologies, and training costs escape the research and research funding processes.

Bruce Judd, associate vice president at San Jose State University, commented on the legal environment. “There are new laws in California that require institutions to notify affected individuals if their systems get hacked and they lose information of a personal and individual nature. Individuals now have legal remedies available that would put the university in a legally liable situation. Security now is mission critical in terms of keeping our heads above water legally.” Mike Adelaine, CIO at South Dakota State University, noted further: “Land grant institutions have to interface with all of the usual campus constituencies, the general public, and many state and federal government agencies. State government particularly has much stricter security policies in place. We need to lower our guard to let our faculty and students conduct their business, but the state government absolutely will not make exceptions. It will be hard to maintain high IT security and open access that is acceptable to both sides.”

The upshot of the legal environment is that tighter technical controls on university systems seem inevitable. “It is likely that our systems are going to be less open to nefarious activities than previously,” predicted Eric Cosens, information systems auditor at Indiana University. “We want to be as open as we can for our educational mission, but higher education is tricky—a balancing act. It’s like walking a tightrope. I’d like to see more intelligent control technologies developed and exploited. Allowing for freedom while having adequate controls in place is the goal.”

Our respondents concurred. A majority (57 percent) agreed that centralized networks and network management were the only way to be able to comply with federal and state requirements concerning IT security. Only 15 percent disagreed or strongly disagreed. Likewise, a majority (66 percent) agreed that standardized networks and network management were necessary to comply with federal and state requirements concerning IT security. Only 9 percent disagreed or strongly disagreed.

Philip Long, CIO at Yale University, provided an interesting perspective on technology as a barrier. “One barrier that is just gigantic is the software that vendors deliver to us, especially in an enterprise situation. We constantly get vendor products that say they have good security. They imagine that we can create a password and net ID for their particular use and somehow their product will exist on a campus as if it were a
stand-alone item.” Jeffrey Schiller, network manager at the Massachusetts Institute of Technology, also noted this issue. “Packaged systems are difficult for us to integrate because they tend to rely on firewalls and VPNs to provide security [rather than incorporating security into the product]. If a vendor says you need a firewall, that’s a warning sign.”

We found no significant differences on the opinions above by Carnegie class or country.

**Impact of Perceived Barriers on Success**

Are perceptions of barriers and success linked? In some cases, yes, but in most cases, no. Respondents who thought institutional security policies posed no barrier to success at their institution rated IT security success and their sense of security higher. We found similar relationships for technology and senior management support.

**Melding IT Security with Internal Business Practices**

A majority (55 percent) of respondents indicated that business requirements take precedence over IT security when the two conflict. Only 17 percent of respondents disagreed or strongly disagreed. This confirms the anecdotal belief that functionality takes precedence over IT security in higher education when new systems are installed. However, respondents who believed security took precedence at their institutions were twice as likely to indicate that their security programs were a success and that they felt more secure than two years ago.

Similarly, most respondents (75 percent) agreed that their institution’s IT architecture and implementation sacrificed some level of protection to ensure ease of use. Only 9 percent disagreed or strongly disagreed.

Some institutions appear to have found an acceptable balance by interwaving IT security with their business practices. Terri Wiskirchen, university risk manager at Embry-Riddle Aeronautical University, noted, “Whenever we look at new systems, new software, or new processes, security is an integral part of the consideration.” At Yale University, Morrow Long believes IT security is woven pretty well into the fabric of business. “In 1997 we built IT security into the new administrative system and into training—how to get accounts, access, and roles and responsibilities,” he said. “HIPAA [the Health Insurance Portability and Accountability Act] forced the medical school to increase information security awareness as well. In research, security is probably not woven as well. Researchers tend to be closed off in their own little worlds. The medical school has done good outreach to the medical researchers to let them know that if they are dealing with clinical or any other personally recognized health information, they have to follow certain privacy standards.”

**Endnote**

Effective Practices and Lessons Learned

People seldom improve when they have no other model but themselves to copy after.
—Oliver Goldsmith

Chapters 4 through 7 described the current state of information technology (IT) security at 435 higher education institutions. In Chapter 8, we analyzed both quantitative and qualitative data to identify factors that appear to affect institutions’ security outcomes. In this chapter, we synthesize what lessons we have learned about the practice of IT security in higher education. A key advantage to surveying hundreds of institutions on IT security is the opportunity to assess what went well and what could have been done better, thereby enabling us to provide valuable insights for the rest of the higher education community. To quote Oscar Wilde, “The only thing to do with good advice is pass it on. It is never of any use to oneself.”

Several common themes emerged from our survey data and in-person interviews concerning effective ways to improve institutional IT security. While many of these insights might sound familiar, their recurrence underscores the importance of incorporating them into our collective thinking about how best to structure and execute IT security activities on our campuses. We recognize that cultures, resources, and technical environments vary significantly across the institutions surveyed in this study and that no single practice described here will necessarily work everywhere. Our data underscore the diversity of our campuses.

IT Security Is Not Just About Technology

While deploying technology is necessary to achieve effective IT security, institutions must place equal if not greater weight on the “soft” aspects of security, including ongoing user awareness; creation of effective, understandable, and enforceable IT security policies; and effective communications, both with the end-user community and within IT organizations. Without such measures, organizations could invest large amounts of money in the latest and greatest technologies but still experience a security breach when users unknowingly employ a weak password, store confidential information on an insecure system, or ignore security policies they don’t understand or consider troublesome.

As indicated in Chapter 5, most respondents in our survey agree or strongly agree that IT security problems inadvert-
tently caused by authorized users are a significant concern. Despite this, nearly two-thirds of the institutions do not have formal awareness programs in place for their faculty, students, and staff. However, in Chapter 8 we showed that universities with awareness programs in place feel more secure than those without such programs. Likewise, Chapter 8 showed us that institutions with formal IT security policies ranked their security programs’ success higher than those without.

These data indicate that nontechnical aspects of IT security can play an important role in enhancing the effectiveness of an institution’s IT security program. As James Bruce, vice president for information systems at the Massachusetts Institute of Technology, stated regarding security awareness and regulations such as FERPA, “People don’t have trouble with the security. They have trouble understanding the rules that mandate the security and how they are applied.” This view is echoed by numerous other IT security practitioners we interviewed.

Gordon Wishon, chief information officer at Notre Dame University, suggested, “Commit resources not only to technology solutions, but to education and awareness—particularly education and awareness among students and faculty and certainly staff, too.” Andrew Conley, network security officer at South Dakota State University, agreed. “You can put all the technology in place, but if you don’t let the users know, a lot of times they can find ways around it or they may do ‘bad’ things unknowingly. User awareness is one of the areas that really needs to be addressed in the security realm.” Jeffrey Savoy, information security officer at the University of Wisconsin–Madison, emphasized, “Your end users are your best firewall. It’s important to get their buy-in on good security practices. They can do important things such as using good pass-

words, updating operating systems, keeping virus definitions updated, and not knowingly circumventing existing security controls.”

Morrow Long, director for information security, Yale University, explained, “Much of your job is not technology and technical. It is people based—working with people, talking to people, dealing with people problems. The most important thing is to communicate well with people. They want to understand what you are saying; if you talk to them in technical jargon, they won’t understand you.” Larry Lidz, senior network security officer at the University of Chicago, said, “There are two main things: convince everyone that security is something they should be concerned about, and build up trust [among the user community].” And according to Beth Cate, associate university counsel at Indiana University, “The more educated Indiana University personnel are concerning security issues and the tools at hand, and ways to minimize risks, the better off we will be.”

**IT Security Requires Senior Leaders’ Engagement**

Involvement of the institution’s senior leadership with IT security is important to the security program’s success. It is difficult to create comprehensive programs and enforce IT security policies without senior academic and business officers’ involvement and support. And it is difficult to convince the university community to conform to those policies without senior leadership’s practicing the policies and articulating the importance of the issues. The institution’s IT security culture needs to change, and that requires the active engagement of the senior academic leadership and faculty governance.

In Chapter 5, we learned that, on average, senior executives are not as involved
in the development of IT security policies as the technology management and staff. However, the analysis presented in Chapter 8 indicated that at institutions where the president or provost was involved in developing IT security policies, respondents felt that their IT security efforts were significantly more successful. Eric Cosens, information systems auditor at Indiana University, explained, “It all starts with the tone at the top. The CIO and campus administration here have made security a priority. The proper tone at the top makes what we do more effective. It is the foundation of the control structure; otherwise, policies are seen as optional and not taken seriously. It has to become part of the institutional culture.”

Engaged and informed senior leadership is also a prerequisite for funding. In Chapter 5, we discovered that 75 percent of institutions considered IT security one of the top three institutional priorities. Nevertheless, we also observed that only 28 percent of institutions agreed or strongly agreed that their institutions were providing the necessary resources to address IT security issues, and 63 percent expected no increase in their staffing levels for IT security, while 17 percent expected a decline. Similarly, more than 50 percent of respondents expect their spending on security hardware and software to decline over the next year.

A significant dichotomy exists between the perceived importance of IT security at institutions and the resources being made available for executing IT security initiatives. One major factor that apparently contributes to this imbalance is the difficulty of engaging an institution’s senior leadership in discussions about IT security and its importance. Chapter 5 showed us that only 11 percent of institutions “often” discuss IT security at senior-level cabinet meetings, and only 17 percent report on IT security “often” to senior management. Because it is often difficult to see whether IT security is working well unless a significant incident occurs, senior management might feel that IT security at their institution is being handled adequately, while those responsible for security struggle to find the necessary resources to protect the institution. Making senior administrators aware of the need for IT security and the issues the institution faces day to day is critical for ensuring that security will be treated as a serious issue—and for getting appropriate levels of funding. This point of view is shared by several of the practitioners interviewed.

“We need to pay more attention to politics,” said Robert Mahoney, team leader for network security at MIT. “In general, the notice of IT security is by its failure, or by some draconian measure that is taken. If you are not maintaining good relationships [with upper management], the only time the word ‘security’ comes up at the highest levels is as a problem.”

Bruce Judd, associate vice president for university computing and telecommunications, San Jose State University, said, “Because I have kept the president’s cabinet as well as the academic senate budget committee apprised with periodic reports on network security and security issues, they now have a greater appreciation of the importance of network security. They raised security funding up to the mission-critical level, whereas before it was viewed as just an option. Now it has the same criticality as the telephone system, the power plant; it is viewed as a utility. I had to do a lot of outreach by laying out the facts and saying things like, there were 280,000 attempts in the last three months to get into our system.”
**IT Security Requires Effective Planning**

In Chapter 6 we noted that 13 percent of institutions reported having a comprehensive IT security plan in place. Forty-two percent had a partial plan in place, 36 percent were currently developing a plan, and 10 percent had no plan at all. IT security threats are continuously changing, and institutions need to be prepared to react to a myriad of new threats as they emerge.

William Paraska, director of university computing and communications systems at Georgia State University, illustrated this point: “You have to have a plan—you have to know what’s out there, what’s going to happen to you, and how you’re going to deal with it. Some schools are out there floundering—without an overall approach [to IT security].” Michael Adelaine, chief information technology officer at South Dakota State University, espoused a similar approach. “We’re trying to be much more proactive than reactive. We’ve sent out a lot more ‘feelers’—trying to look in those dark, deep Web sites where chats occur to get a sense of the drumbeat that goes on out there. We set up a plan as to how we were going to deal with a potential cyber attack. We have firewalls and a whole host of systems there. But as far as the human element, we’re out scouting the territory to see if there is trouble on the horizon, where it might affect us, and then we develop a plan. Before, we just hoped our technologies were in place.”

Jeffrey Schiller, network manager at MIT, gave a more concrete example of how effective incident response procedures can impact an institution’s ability to react to a new threat. “We have a very effective incident response team. The fact that we can say we had zero to one Code Red [worm] infections on a campus this size [shows the importance of a strong incident management capability].”

**IT Security Requires Diligent Monitoring**

We cannot overemphasize the importance of monitoring institutional networks and systems for abnormal activity. Regular monitoring for abnormal activity helps institutions quickly identify incoming attacks, locate and isolate machines with known vulnerabilities, or react to security breaches in process, such as a PC infected with a worm. On the basis of our survey research, higher education appears to be doing a relatively good job of monitoring its systems. Sixty-six percent of respondents indicated that they monitor their networks daily, 54 percent monitor their operating systems daily, and 59 percent monitor their enterprise systems daily. Fewer than 15 percent of respondents indicated that they do not monitor these components regularly. However, only 58 percent of respondents indicated that they conduct regular and frequent scans to detect known security exposures in their critical systems, and only 39 percent agree that they conduct such scans for all university-owned systems connected to their networks. Our respondents described several different monitoring approaches.

Philip Long of Yale University said, “We license the ISS scanning system and do a campus-wide scan of all campus computers for vulnerabilities on a periodic basis. We collect them in ways that make sense and forward them to the systems’ administrators of record—for those systems for which we have records. That is actually quite an educational experience for those people. Our security team is called from time to time to do security assessments of various kinds of systems; we will run the scans on the system and give advice for free. We will
not remediate for free; we are a charge-back operation.”

According to San Jose State’s Bruce Judd, “A lot of the monitoring tools we use are not expensive, as they are open-source tools. We take advantage of open-source tools, so the cost of what we implement is really the cost of the hardware, not the cost of software and software maintenance. There are some wonderful open-source tools: Big Brother and Cricket, for example. It is acceptable to use open-source tools for monitoring.”

MIT’s Robert Mahoney described a different approach to intrusion detection. MIT runs an open network without a perimeter firewall. This causes a problem, since “a lot of [intrusion-detection systems] products assume you are behind a firewall, and so, if you see something, it has penetrated your firewall and must be important.” MIT’s approach is to “mostly focus on outgoing attacks, which either represent a compromised machine or malicious behavior, and we rarely see a malicious attack [originating from here].”

**Work With, Not Against, Your Constituents**

In academic environments, particularly large research institutions, many constituent groups on campus often suspiciously view the IT security team as “Big Brother.” This perception is sometimes enhanced when institutions take an overly aggressive posture toward enforcing campus policies, thereby encouraging people or departments to find workarounds rather than comply. MIT has shared some interesting techniques for working with its campus communities to enhance security compliance.

MIT has developed a sense of community around IT security by creating a virtual IT security team staffed by two central IT full-time employees but also enlisting volunteer participation from nearly every school and major research laboratory on campus. By allowing and encouraging broad participation in IT security efforts, MIT gains consensus for broad-reaching IT security decisions while leaving each unit enough autonomy to deal with security issues in ways best suited to its individual environment.

According to Michail Bletsas, director of computing at MIT’s Media Lab and one of the volunteers contributing to MIT’s security team, “It [the security team] is extremely effective. I think it was one of the most successful efforts ever in IT here. We have never had to shut down our connections. For example, the SQL Slammer [worm] was dealt with in six hours, and that was on a Saturday night. There are a lot of smart volunteers who contribute to the cause.” Bletsas continued, “The more of us who play this role, the better it is for the university. I wouldn’t want to substitute the broad consensus that exists right now with the network security team with a rigid set of rules. This is a very fluid field right now, and one of the worst things you can do is set up rigid rules that everyone has to abide by.”

MIT also takes an interesting approach to confronting its constituents regarding IT security issues. According to James Bruce, “If you went to Johnny and said, ‘You did thus and so,’ he would deny it. If you say, ‘Someone is using your account to do thus and so,’ you will typically get an apology, and the activity will cease.” MIT takes this approach to notifying its users about violations of the institution’s IT security policies, and it has proven effective. Bruce said that over many years they’ve only once had a three-time offender who had to be referred to a disciplinary committee.

Jeffrey Savoy of the University of Wisconsin–Madison noted, “At a decentralized campus, controlling devices connected to the network is a challenge. Our process is that when a computer is hacked, it may be
taken off the network. Then, it will have to be audited by central security staff before it can be put back on [the network]. Repeat offenders have to go through a more thorough consultation with central security staff. First, we explain what we’ve done and then we explain how their compromised machine puts their campus colleagues at risk. We also educate the offender about what to do to prevent the compromise in the future, and most importantly, we obtain a commitment from them to perform the necessary security activities in the future.”

Several research universities also noted that it is sometimes difficult to get faculty members to comply with security regulations, which, for example, require a compromised machine to be removed from the network until it is repaired. Philip Long described this situation and what Yale is doing to address it: “The most difficult situation is the researcher who is trying to get the research application in by the deadline the next morning and his machine is hacked into the night before. We block it from the Internet and he is upset because he says getting his grant application out is more important than protecting the network from a virus or hacker situation. But we are very sympathetic in that situation. We find a way to bring up his machine behind a firewall—we will bring up his machine behind it and let him relay what he needs to the Internet through this trusted machine—but we are not going to let his hacker on the network using his machine while he uses his machine to finish his work. We will also bring up the machine in a controlled environment, and he can copy files off of it.”

Long, along with others who reported similar situations, indicated that this case is the exception rather than the norm. “More often what happens is that people will remediate their machines within 24 hours, because who wants to be off the network? We call up people to inform them that there is a high school student from Toronto, Canada, logged into their machine and he is using it to mount a denial-of-service attack on Los Alamos, and they go, ‘Oh my God!’”

**IT Security Requires New Incentives**

Numerous IT security administrators we interviewed cited user adoption of IT security tools and techniques as an issue, especially at larger institutions where decentralization limits the direct control the central IT group has over systems and networks run by departments, schools, and researchers. These IT security professionals believe users generally want to help the institution to be secure but are often unsure how to do so. Another commonly held opinion among the IT security community is that end users’ willingness to be secure is only good up to a certain point. If asked to do too much, in terms of either effort or knowledge, they will not readily comply.

Given the university community’s apparent willingness to act securely if it proves convenient, institutions can take several approaches to make it easier for their users to behave in a secure fashion. Some of these are simple and low cost, whereas others require more effort to implement and maintain but also promise better returns. As Gregory Jackson, vice president and CIO of the University of Chicago, explained, “The more you make it easier for people to do the right things, the more successful you will be.”

One simple approach is to create easy-to-follow instructions (or link to someone else’s instructions) to secure commonly used systems and applications and make them easily available on the Web. Remind users that the updates and instructions are available, especially when a new operating system version is released or a new vulner-
ability is discovered. Similarly, institutions can create easy-to-understand versions of key security policies, along with IT security FAQs, and make them readily accessible to the community. The University of Texas at Austin has created such a site at <http://www.utexas.edu/computer/security>. It provides tips geared for both individual users and system administrators to help them secure their systems, and it has copies of all the institution’s IT security-related policies in one place. The site also provides news on new security issues and a form for submitting questions to the university’s IT security staff.

Another relatively simple approach is to provide links to commonly used IT security tools such as antivirus software, personal firewall software, or secure communications tools like SSH or SFTP from an internal Web site, making them easy to find and install. Many of the campuses we interviewed have site-licensed commercial applications like antivirus software and make them available to all users at no charge. By making it easy and cheap for users to find and install these applications, institutions substantially increase the chance that they will be used. Stanford University has developed such a site for its community at <http://www.stanford.edu/dept/itss/ess/>.

A somewhat more complicated approach is for the institution to create its own installers for commonly used operating systems and applications with all desired security modifications included and distribute them to campus system administrators and users on either an intranet server or physical media such as CDs. Another approach is to provide this type of “hardened” load-set on computers purchased through the campus computer store or a negotiated preferred vendor program. Tufts University has taken this approach, providing a customized load-set that includes institution-specific security templates through a vendor agreement with Dell. Details on this program can be found by going to <http://ase.tufts.edu/its/tech.htm> and clicking on the “Dell Special Pricing” (department pricing) link.

Another, more complex, approach uses automated system configuration tools to monitor individual systems’ configurations and automatically push updates out to them as necessary. This approach takes responsibility for at least some aspects of security management out of users’ hands. This solution is common in the corporate world and is sometimes used in public computer labs at universities to ensure that systems remain configured as desired. However, its use does not appear to be widespread in higher education, perhaps because these are commercial systems requiring an upfront investment to purchase, or perhaps because the diversity of systems found at most colleges and universities makes the use of such a tool unwieldy. It might be feasible for institutions to consider an approach by which departments or individual users could sign up with central IT to participate in such a program, in return for a system management fee that would cover the program’s cost. The institution could limit the operating systems and applications supported to make the program easier to manage.

A more resource-intensive version of the previous approach is for central IT to provide system management services on a charge-back basis to departments they don’t normally support, as at least one institution we interviewed is doing. By taking this approach, they ensure that departments without access to professional IT support can have their systems managed by competent staff, reducing the institution’s risk while leveraging their staff in areas like the help desk.
By implementing one or more of these suggested approaches and lowering the barriers for users and departments to make themselves more secure, institutions increase the likelihood that their community will make more of an effort to secure their systems and applications, increasing the level of security for the institution as a whole.

**Differences of Opinion**

While the above lessons contain opinions shared among most institutions we interviewed for this study, we also noted several IT security areas where opinions differed on the appropriate course of action, even among leading institutions of similar size, mission, and complexity. This section expresses these differing points of view.

**Firewalls**

Using perimeter firewalls as a first line of defense against potential cyber-miscreants has become the norm in most industries; the CSI/FBI 2002 survey shows 99 percent of respondents using firewalls. As shown in Chapter 4, only 70 percent of higher education institutions are using perimeter firewalls. However, for at least some of the institutions not using perimeter firewalls, this is not a lapse in security but rather a conscious strategy.

MIT’s James Bruce expressed the “no perimeter firewall” view. “This is a university. For us, this means that the network pretty much has to be an open network. And so we pretty much don’t believe in firewalls. The enterprise networking environment has no firewalls in it. Some departments will run firewalls—for example, genetic data and things of that nature—and the Lincoln Laboratory, which is part of the MIT address space, has a firewall, but for the most part, since our researchers like to explore new protocols, port assignments, and new applications, trying to build a firewall is a fruitless endeavor. Just as soon as you build one, somebody wants to do something different, and you keep punching holes in it, and after a while it looks like Swiss cheese. So that means for us that the fundamental proposition is that our computers and our applications need to be secure. We focus on security at the individual machine level. We worry a lot about operating system security, about the bugs in operating systems, and we focus a lot on ensuring that our applications have appropriate levels of security, so indeed, we know who is making the transaction when the transaction occurs. We encourage people with computers to keep their operating systems at the current release and to make sure that all security patches have been applied.”

Institutions like the University of Washington hold similar views. Other large research institutions, such as Indiana University, are beginning to evaluate perimeter firewalls but have not yet implemented them.

On the other hand, numerous institutions have installed perimeter firewalls and are pleased with the results. Paul Howell, information systems security officer at the University of Michigan, sees firewalls as one of the most effective IT security technologies an institution can deploy. “If you can install them and operate them correctly, they tend to be the key thing to go after because they tend to keep undesirable traffic from the Internet [from] washing up on your machines, [and] that can cause a lot of headaches.”

San Jose State’s Bruce Judd said, “You have to secure the network in two places—the core and the border. If those are well secured, then you can usually deal with everything in between.” He continued, “[On our campus], every server and system service has to be registered with the firewall. Other servers are on private and unroutable
network segments. Now the only way you can get into a server in this private address space is through a VPN.”

South Dakota State’s Andrew Conley said, “We felt implementing the firewall is really effective because on our campus it blocked out a lot of people and scripts who are out there scanning. This approach has led to the biggest improvement of IT security at our institution.”

Analysis presented in Chapter 4 showed that the larger the institution, the less likely it was to have implemented a perimeter firewall and the more likely it was to use an interior firewall. The examples provided above suggest that campuses need to decide whether perimeter firewalls are a good fit for their culture and IT support capabilities.

Those who oppose perimeter firewalls feel they restrict their constituents’ ability to make free and open use of the campus network. However, to provide security, this approach needs to emphasize stronger measures at the individual system level, shifting the burden of support somewhat away from central IT and toward departments and individual users. On the other hand, installing firewalls requires IT organizations to be responsive to changing user demands and may also require awareness efforts, because having a firewall can sometimes cause lax security behavior among users. Either approach can provide adequate security, but one approach or the other may be a better fit for a particular institution’s needs.

Policy

Institutions also have slightly differing opinions about the need for IT security policies and how comprehensive they need to be. As reported in Chapter 5, nearly 70 percent of responding institutions either have or are implementing some form of formal IT security policy, and only 8 percent of institutions report that they have no IT security policy. We noted some opinion differences about what these policies should contain.

Indiana University is a good example of an institution with strong emphasis on IT security policies. Indiana has about 20 policies that cover IT security in some way. Its Information Technology Policy Office is responsible for creating and reviewing IT policies and educating the institution’s constituents about them.

Numerous institutions have not emphasized policy so much as part of their IT security efforts. When asked to describe his institution’s IT security policies, MIT’s James Bruce said, “MIT historically, and almost by intent, has fewer policies [in general] than most universities have. You will find some very simple network rules of use. However, more is done through [user] awareness than through policy.” The University of Washington is currently working on implementing its first formal IT security policies, although interim policies created by the IT organization have existed for some time.

While our analysis in Chapter 8 showed that having IT security policies does seem to make a difference, our survey research did not uncover the nuances of whether these policies were comprehensive (as at Indiana University), general (as at MIT), or unofficial (as at the University of Washington). From those institutions we interviewed for this study, we gathered that the decision as to which IT security policy route to take is largely cultural. If your institution tends to be policy driven, your IT security efforts will likely be more successful if you have strong, enforceable IT security policies. At an institution that is more policy averse, having strong IT policies may not be possible, and other approaches may need to be considered.
Since the first host computer at UCLA was connected to the ARPANET in 1969, both J.C.R. Licklider’s vision of a “galactic network” and the practice of internet networking have rested on principles of openness and accessibility. The Internet’s earliest engineers at our colleges and universities built the current Internet following these principles. And much of what we have described in this study is the product of more than three decades of engineering and evolution guided by these principles. Openness and accessibility are at the core of higher education’s Internet practice, regulation, and engineering. We can summarize this practice for most higher education institutions as follows: unfetter the Internet, rely on local policy and behavioral awareness, and secure the end points (desktops). The open Internet approach aligns well with the ideals of a democratic society, and certainly with those of higher education.

Today these principles and the open Internet are at risk because of increasing, persistent, and ever more malicious attacks on our networks. A major debate is commencing among information technology (IT) security professionals focusing on these principles’ merit and sustainability in the current environment and whether new or modified principles need to be adopted. Openness and accessibility are recognized as major factors contributing to the Internet’s power to foster innovation. But increasingly they appear to place Internet security at too high a risk. Also, an open system depends on widespread awareness and behavioral self-controls on the part of network citizens. The current level of awareness and IT security practice on the part of the constituency does not appear to be commensurate with the current level of risk, leading IT security professionals to aggressively use available technologies as countermeasures. A new alignment of IT security with higher education’s values, practices, and installed technologies may be needed and may already be occurring.

In a presentation entitled “Security in the Post-Internet Era,” given at a workshop in Chicago on 12 August 2003, Terry Gray, director of networks and distributed computing at the University of Washington, squarely engaged this debate by offering a controversial thesis: “The open Internet is history, get over it.” Gray based this assertion on...
the observation that two recent Microsoft security vulnerabilities have forced most institutions and ISPs to embrace blocking of selected network services. Comcast, a major cable provider, has, for example, started blocking NetBIOS ports and is now blocking ICMP/ping. Almost everyone is now blocking the NetBIOS ports, if they weren’t previously. In some Comcast areas, VPN (virtual private network) ports are also being blocked. On some campuses, there are frustrated, and probably exhausted, network administrators who favor blocking ports forever, contrary to their earlier and long-held belief in removing blocks.

Gray concluded that the new widespread vulnerabilities, combined with increased liability concerns, have brought us to a turning point, even in higher education. To his thinking, insecurities equal liabilities, which in turn will trump the concerns of network operators and users. Gray also argued that restrictive access policies resulting from these insecurities may impede innovation, the lifeblood of any college or university.

A fundamental shift in policy and practice toward a less open Internet will have profound implications for scholarly communications in higher education and IT security practices in colleges and universities. A key question is whether institutions can meet contemporary security requirements without undermining innovation, that is, whether innovation can find a way to flourish in spite of restrictive connectivity policies. If Gray is right, the pressure on the academy to align its values and beliefs with mainstream IT security practices will become irresistible. Some believe that academic values are inimical to IT security practices, and we will elaborate on these perceptions or “myths” about IT security on the basis of the study’s findings. Gray’s conclusions suggest that the moral exchange of scholarly ideas, right or wrong, are moot if they conflict with security requirements.

While the impulse to lock things down through unprecedented technical interventions is easy to understand amidst the mopping up of more than 150,000 infected machines in July 2003, there remain many advocates of continued openness on the Internet. Some, like Ken Klingenstein, project director of the Internet2 Middleware Initiative and chief technologist at the University of Colorado at Boulder, argued that a trend toward an Internet with only a few ports open and lots of other applications tunneled through those ports (port 80) is unsound policy and technically questionable. The debate is far from over.

In anticipation of IT security practice changes, we use our findings to suggest ways that higher education practitioners can align IT security with institutions’ needs in this ever-changing environment. We elaborate on the changing environment and future trends that can be reasonably ascertained from our research. On the basis of these data, we suggest effective practices and strategies that build on the assumption of an open Internet. We also acknowledge that this key assumption may not be sustained.

**IT Security Beliefs in Higher Education**

This section presents some of the most commonly articulated beliefs (or leitmotifs) that create tension or operate as barriers to improving IT security in higher education. We look at both sides of arguments surrounding these beliefs. We present counter-arguments that practitioners may be able to use at their institutions to overcome these barriers, whether they are indeed barriers or simply myths.
IT Security Inhibits Academic Freedom

One of the most frequently heard arguments against implementing stronger IT security at higher education institutions is that strong IT security is inimical to academic freedom. The concept of academic freedom embodies the right of faculty members and students to pursue controversial topics without censorship or the need for prior approval. The academic community needs open and unfiltered access to information resources to perform their teaching and research. There is a widely held perception that having strong, centrally managed IT security will somehow impinge upon this freedom.

Those who espouse this point of view seem to have several major tenets to their argument. First, they feel that having security in place would block their ability to do something, such as accessing resources or using a new technology. Second, they feel that by having to authenticate to the resources they access, their usage may be tracked and used against them in some way. Third, some feel that as academics, they should not be subject to standardization, regulation, or inconvenience when accessing institutional resources, including IT.

The viewpoint that IT security blocks access to resources, invades privacy, or introduces complexity or regulation likely derives from IT security technology, policy, and procedure implementations that are poorly aligned with the academic community's needs. It is certainly possible to create an IT security environment that introduces all of these problems and more. However, it is equally possible to create an environment in which IT security takes the academic community's needs into account.

If properly implemented, IT security can enhance academics’ ability to access the resources they want to access, when they want to access them, with little fear of being monitored. For example, an effective IT security program ensures access to institutional computing resources by preventing denial-of-service attacks, infection by computer viruses and worms, or other damage caused by hackers. It helps protect the data resident on institutional computers, thereby protecting the privacy of students, professors, and researchers by preventing unauthorized people from viewing their work or learning what information they have been accessing; and it ensures that their research is kept safe.

Technology alone is not the solution to creating such an environment. As with most complex technology implementations, policies and business decisions made when implementing the technology will dictate the results achieved. A firewall can be used to prevent all contact with the outside world or to limit the traffic that is allowed to pass through to an administrative computer, simultaneously leaving machines used for academic purposes largely open. Enlightened policies and procedures contribute to user confidence that academic freedom is being respected. Informing the academic community about IT security policies and demonstrating that the policy is being followed and can be trusted can alleviate many concerns about security's negatively impacting academic freedom.

We note that although academic freedom was the third most frequently cited barrier to IT security among our respondents, only 32 percent selected it as a barrier from a “choose all that apply” question format. This suggests that while this argument may be popular, most institutions may have figured out a way to work around or accommodate this concern.
IT Security Compromises
Personal Privacy

Another commonly heard complaint about IT security is that it compromises personal privacy. In particular, when use of an authentication technology is required to access institutional resources, students and faculty fear that data is being collected on their activities and may later be used against them.

While tracking individuals’ activities through their interactions with electronic systems has become endemic in today's society, ranging from the location of mobile phone calls to the use of ATM machines to the purchase of individual items at grocery stores, technology is just a tool that enables such tracking. Use of technology does not mandate that user information be tracked or that it be shared. Such decisions are driven by an organization's business needs, culture, and policies.

In many cases, the institution's business needs dictate that certain activities be tracked to ensure that institutional systems and information assets are being protected. For example, logs are kept of access to secure areas of the campus, if electronic keys are being used, to allow campus police to determine who was in a particular facility when a crime was committed. Log files are kept of changes to information such as student grades or financial transactions to protect against fraud.

However, organizations can take such tracking beyond what is necessary for business purposes. For example, it may be necessary for copyright protection to validate that a user trying to access an electronic publication is an active member of the university community prior to permitting access. But the institution has no reason to track the fact that a student is reading a right-wing political journal on a regular basis or that a foreign professor seems very interested in articles about terrorist tools. Also, an institution probably has very little reason to track what Web sites a particular user has visited using a university network connection, although the capability to do so certainly exists. In situations where the business need is to determine whether a user is legitimate, we expect that most higher education institutions, rather than monitoring usage, will err on the side of collecting less information, to allay privacy concerns.

Again, having an accepted policy that explains what information the institution collects on its constituents, what the information will be used for, and when it is discarded can calm fears of the user community. And a well-conceived policy can prohibit an overzealous administrator from collecting information that does not enhance the institution's security but could compromise individual privacy.

A policy cannot be effective by itself. The institution must conduct awareness activities for users to ensure they understand and trust the policy and for staff members who configure and use security technologies. To further build confidence, the institution may wish to periodically audit the information being collected on its users and require business justification for any storage of personally identifiable information.

A close parallel to the issue of electronic surveillance and privacy exists in the library. Every time a library patron borrows a book, data linking the borrower and the book must be collected and stored until the transaction is completed and the book is returned, to ensure the university gets its book back. Does the library use this information to maintain records of what books individual students or faculty members have borrowed during their tenure with the institution? The library certainly has the capability to do so. Perhaps because this process has been around much longer than IT security tools, users are more
accepting of it, or take it for granted that their privacy is being protected. However, one does not often hear academics bemoaning their loss of privacy in the library, yet such cries can be heard in the IT security arena.

**IT Security Limits Access to Information**

Some users see firewalls, strong authentication technologies, secure application versions, and similar technologies as blocking access to online destinations, limiting their ability to collaborate with colleagues at other institutions, or restricting the technologies they can use. For example, our data show that 33 percent of baccalaureate institutions and 17 percent of doctoral institutions block some URLs through their firewalls.

Morrow Long, director of information security at Yale University, described Yale’s approach to this issue: “When we close off access, we try to make sure it is not in conflict with the academic and research purposes of the university and the missions of the university. We have blocked off some things like Windows file sharing in the Internet for security reasons. We were very careful to publicize our decision and to obtain input from all members of the community. We made an alternative available to people who wanted to access PC hard drives from the Internet via a VPN. When we implement security, we try to make sure that it does not impede or impinge upon anything that people are doing or make sure that they have a chance to comment on it.”

As with many other aspects of IT security, technology is only part of the picture. Configuration decisions and institutional policies and procedures play a much larger role than does the technology itself in determining whether deployment of a particular technology will cause users to lose access to some resource. Likewise, the purpose for which a technology is deployed will largely determine how it affects users and their work. For example, a tightly configured firewall deployed at the perimeter of a research university’s network might overly restrict some users’ ability to access resources they need, yet the same device deployed to protect a particular network subnet hosting the university’s administrative systems would have no such impact. Institutions that work with their communities to define solutions find that in many cases they can adequately balance the need for security with users’ business needs.

**Openness and Community Outreach Are at Odds with Security**

The open sharing of information, both within and beyond the institution’s walls, is part of many colleges’ and universities’ core mission. This need for openness often arises as an argument against adopting stronger IT security measures. Advocates of this position contend that security technologies would block their ability to share information within and beyond the institution.

When configured in a way that is aligned with the institution’s academic and business needs, IT security tools and techniques should have minimal impact on the ability of faculty and students to openly share information with each other, with colleagues at other institutions, and with the world at large. We must ask, then, what exactly are we currently making available that we wouldn’t be making available if we were more secure? In nearly all cases, the decision to implement stronger IT security will not change the types of information being made available, unless someone deems that particular items (such as research on biochemical agents) may only reach a restricted audience, given the data’s sensitive nature.
Although institutions shouldn’t need to significantly change the types of information shared and collaboration tools used, they might need to change how these activities are performed. For example, incoming Web traffic might be restricted to a certain set of servers for security purposes, requiring faculty members to publish their information on centrally managed Web servers rather than from departmental machines. Similarly, an institution might require that users employ secure versions of certain applications, say, SSH instead of Telnet, or SFTP instead of FTP, thereby providing a more secure environment without changing the functionality available to the end users.

**A Transient Student Population is Difficult to Manage**

Some believe that the “transient” nature of higher education’s constituents complicates IT security management. Because a student’s association with the institution often has a fixed duration, it is assumed that managing user accounts for a population with 25 percent or greater turnover per year is more difficult than similar tasks in other industries. Likewise, it is assumed that getting students to understand and comply with security policies and best practices is an ongoing and often futile effort compared with similar efforts in industry.

In reality, the issues faced by higher education regarding end-user turnover are similar to and may be easier to manage than those faced by industry. Although a transient population, students’ tenure with the institution is predictable. Security staff can plan for a large influx of new users in late August or early September and assume they'll need to shut down a large number of user accounts after graduation each year. The user accounts affected by these changes are easily identifiable, and many institutions have developed automated tools to let students activate their user accounts. Also, user account privileges for students tend to be very similar, making it easy to give students access to the systems they need. Some sectors of industry also face turnover rates of 20 percent and higher, but, unlike in education, such turnover is often less predictable and requires immediate termination of access rights, as the departing employees may have been fired or be leaving to go to a competitor.

A remaining issue is the institution’s ability to get student users to comply with security policies and best practices. As we noted in Chapter 7, some institutions require that students read and prove they understand a simple set of acceptable use procedures before they can activate their user account. Others limit the institution’s exposure to security vulnerabilities on student-managed machines by using firewalls for the residence halls, separating them from the rest of the campus network.

**Faculty Autonomy Can Hinder Uniform IT Security Standards**

Faculty members at colleges and universities are well known for their autonomy. The central administration at many institutions may have difficulty compelling their faculty and researchers to conform to rules and standards, particularly when some faculty perceive that such standards could impede their work. Moreover, at larger institutions, individual schools and even departments may operate with a significant degree of autonomy. Mark Yudof, former president of the University of Minnesota and now chancellor of the University of Texas System, once quipped, “Being president of a university is like being the managing director of a cemetery. You have a lot of people underneath you, but nobody listens.”
Some institutions may have created IT security standards without regard for faculty needs, perceived or real. For example, requiring users to change passwords on administrative systems every 30 days works fine for staff members who use the system every day. But a faculty member who only accesses the system to enter grades once per semester probably sees such a policy as an imposition. Many faculty members value their ability to control the systems they use in their research and need flexibility to change their computing environment when necessary. Trying to fit such requirements into a framework designed for a corporate or administrative environment would be difficult at best.

To introduce security standards, IT security personnel must work with faculty members and their staff to make them aware of the need for security technologies, as well as their capabilities and limitations. They must design and implement standards flexible enough to accommodate both academic and administrative needs. This may be accomplished by setting broad standards such as “every computer connected to the network will run antivirus software,” rather than trying to dictate a particular brand and version. Thus, autonomous individuals or departments can develop solutions that best fit their needs.

Several respondents suggested facilitating IT security standards adoption by making it easy for autonomous users and departments to access centrally provided secure resources. For example, numerous institutions license antivirus software and make it available at no charge to the university community. Although users are not required to install this software, it is easier and cheaper than pursuing another alternative, and usage rates are high.

Using a slightly different approach, one institution centrally deployed Kerberos and digital certificates for authentication purposes. Although the Kerberos principal was linked to the university's central e-mail system, IT security personnel found that some users were not using their university-provided e-mail and therefore were not taking advantage of the additional security provided by the Kerberos/certificate-based authentication architecture. Many users didn’t know this technology was available or what its benefits were. To broaden its usage, the institution began requiring the use of a Kerberos principal to authenticate to critical business applications such as course registration or benefits enrollment. This substantially broadened Kerberos usage on campus without mandating that users employ a new technology just for security’s sake.

The Kerberos example also illustrates another key point about end users’ adoption of IT security tools and techniques. The easier the technology is to acquire and use, the more likely users are to adopt it. The ideal IT security environment would be nearly transparent to the end user, providing utility-like ease of use. Achieving such a level of transparency while providing adequate levels of security for the institution’s perceived risk level would mitigate many barriers to adoption of stronger IT security on our campuses. Through use of middleware technologies such as enterprise directories and role-based security, which enable easy-to-use features like single sign-on, institutions will be able to move closer to providing a more secure environment that their users will be willing to use.

**Common Themes**

In examining beliefs about IT security in higher education, we observed some common themes. First, some members of the academic community believe it is possible to deploy IT security tools and techniques in ways that cause problems for the university community, and, given the often broad ac-
ceptance of this belief, a good number of IT organizations probably have done so in the past. More important, however, with proper planning and design of IT security initiatives that take both the academic and the business needs of the university community into account, these myths do not have to become reality. As we have pointed out several times in this study, nontechnical factors including leadership, policy, education, and trust are essential components of an IT security architecture designed to protect and enhance rather than hinder a user’s work at the institution. We also believe IT security discussions need to be conducted in layman’s terms and focus on its impact on users as much as, and perhaps more than, its impact on the institution. And the discussion should involve representatives from all sectors of the institution.

Aligning IT Security with the Institution’s Needs

Throughout this study, we have presented evidence that IT security is not just a technology issue. To be effective, IT security needs to encompass a strategy that is aligned with the institution’s academic and business needs. Such a strategy needs to include the use of strong IT security technologies balanced with the people side of security, including strong leadership, effective policies and procedures, and awareness and training activities. Every institution has different needs, different resources, and a different starting point. Institutions must understand what threats they feel they need to protect against and develop an IT security program that addresses these threats in a way that does not adversely impact their constituents. This section presents some strategies, tools, and ideas that may prove useful to institutions starting down this path.

Balancing the Technology/People Equation

Our analysis indicates that many of IT security’s “soft” components—leadership, policies and procedures, and training—have an appreciable impact on the perceived effectiveness of IT security. However, our research also found that many institutions focus much more on IT security’s technology aspects than on the people side. When asked to describe their institution’s IT security initiatives, many people we spoke with went into great detail about their firewalls, authentication tools, monitoring and scanning tools, and other technologies they had implemented. In most cases they gave fewer details about how awareness was handled or how policies and procedures were created, followed, and enforced. As presented in Chapter 8, when we asked survey respondents to identify barriers to implementing effective IT security at their institutions, only 10 percent pointed to technology, while awareness, for example, was an issue for 46 percent. In Chapter 5, we discovered that only 54 percent of respondents had formal IT security policies, fewer than 20 percent of institutions reported “often” to their senior management on IT security issues, and fewer than 40 percent had awareness programs in place for faculty, students, and staff.

On the basis of this evidence, we see an imbalance between IT security management’s technical and people aspects at many institutions. While this is not quantifiable on the basis of the data collected for this study, our qualitative research suggests many institutions may be dedicating the bulk of their IT security resources to implementing and managing the technical aspects of IT security and allotting far fewer resources to managing the people aspects. However, the analysis presented in Chapter 8 indicates that institutions that have emphasized the cultural aspects of IT security management
feel that they are doing significantly better in managing their institution’s IT security risks than those that have not. Although technologies are certainly an essential part of IT security, our analysis points to a need for institutions to strike more of a balance between technology use and people-oriented tools and techniques to make their IT security programs more effective.

**Balancing IT Security Approaches**

Figure 10-1 graphically depicts the issue of balancing technology and culture to create a balanced IT security approach. It shows four major strategies for securing an organization on the basis of the organization’s strength in each area.

**Reactive.** A reactive organization will tend to have invested relatively little in either IT security technology or culture. This is not to say that the organization has left itself wide open to all threats, but it has not implemented a full spectrum of leading-edge technologies or leading practices for creating a secure culture. An organization pursuing this approach is likely to invest in IT security on the basis of incidents rather than as part of a strategic plan.

**Cultural.** Organizations emphasizing a cultural approach to security focus their efforts on creating a culture of security. By instilling awareness of security issues into their workforce, creating and disseminating comprehensive policies and procedures, and training their users, they hope to be able to avoid the many security vulnerabilities caused by human error and limit their investment in technology.

**Technology-centric.** This approach relies primarily on technical means such as firewalls, scanning tools, intrusion detection systems, and other technological solutions. It is focused on the prevention and detection of security breaches through technological means.

**Fortified.** Fortified organizations are those that have a balanced approach to IT security, combining both technological and cultural elements. They invest in both technology and culture, recognizing the importance of both in creating a secure environment.

---

![Figure 10-1. IT Security Approaches](image-url)
systems, and complex authentication and authorization systems to secure IT assets. Highly decentralized organizations or those without strong executive sponsorship may be more likely to use such a strategy.

**Fortified.** A fortified strategy encompasses both strong IT security technology and a security-oriented organizational culture. Organizations using such a model will generally do so as part of a conscious plan, as this approach would be difficult to arrive at through an evolutionary path. Those choosing such a model probably tend to do so because they perceive themselves to be at high risk from IT security issues; because some external requirement, such as HIPAA (the Health Insurance Portability and Accountability Act), has led them there; or because security is a concern for one or more of their senior executives.

Note that this model is not intended to be prescriptive. An institution might find any one of these strategies appropriate, depending on factors such as perceived risk, available resources, institutional culture, and executive leadership. Also, these strategies are not absolute and can be pursued to varying degrees. So, for example, an institution choosing a reactive strategy could choose to be technically reactive (farther to the right on the technology axis), culturally reactive (closer to the top on the culture axis), or balanced (toward the center of the diagram). We feel that regardless of the strategy chosen, many institutions will move toward a balanced approach, represented by the shaded circle in the diagram’s center, because such an approach offers a good mix of effective technical and cultural solutions to IT security issues while limiting the resources needed to execute the strategy. Also, the more balanced the approach, the more likely it is to align with the institution’s academic and business needs.

Today, we feel that many, although not all, higher education institutions are in the technology-centric quadrant. Several factors may account for this. First, IT security does not appear to be high on most institutions’ executive agenda: fewer than 40 percent of responding institutions had a neutral or better opinion that their president or provost participated in the creation of their IT security policies, and fewer than 15 percent frequently reported on IT security to the institution’s senior management. Fully 95 percent of our respondents indicated that IT security reported to the CIO or other IT manager.

Without strong executive support, IT security organizations often find it difficult to get their constituents to pay attention to training and awareness efforts, to set standards, or to enforce policies. As one senior IT security officer at a large research university stated, “The problem we have with [IT security] education around here is getting people to pay attention. Communication in our environment is very difficult, because we have many vehicles for communication, and people can ignore them all.” And because IT management has responsibility for IT security initiatives, they may tend more toward the known realm of technology solutions and less toward the more difficult cultural approaches.

A second major factor contributing to higher education’s technology-centric bent may be the availability of resources to manage and enhance security. Every organization must implement a certain degree of technology (such as authentication and virus protection) to adequately protect its users and assets from common threats, and in some cases, resources may not be available to progress far from this baseline.

As described in Chapter 8, nearly 72 percent of respondents cited resource availability as a barrier to IT security at their
institution, and this view was backed up at many of the institutions interviewed as part of this study. As one IT security officer said, “We’re in a time of budget reductions, and it is hard to make the case [for more people]. Without the people, customer service will suffer first.” Carol Myers, director of ITS Security Services at the Maricopa Community Colleges, concurred. “Our technical work has been more successful than our training and awareness [activities]. We lack the budget for them.” When asked, “If you received additional resources for IT security, how would you invest them?,” many IT security managers interviewed indicated that they would like to invest more heavily in user awareness and education and to make their institution deal more proactively with IT security issues.

Understanding and Managing Risk

Illustrating the need for a balanced IT security approach, Figure 10-2 presents one simple model for evaluating the types of security risks an institution could face and outlines some common approaches used to combat each type of threat. Note that for clarity, the figure omits approaches that could be used against all threat categories, such as authentication and authorization tools and antivirus software.

Using this model, institutions could address four different risk categories.

**Internal and accidental.** This category encompasses internal users’ unintentional security breaches, such as using a blank or easily guessed password, storing confidential data on an insecure system, or giving out their passwords to someone over the phone. Such security breaches are difficult to combat because automated tools cannot easily prevent human error. To mitigate these risks, institutions need to develop policies and procedures to guide internal users as to what they should and should not do in...
particular situations, train users on these policies and procedures, and continually offer awareness activities to ensure that users are conscious of new threats and will remember to act securely.

**External and accidental.** This somewhat rare type of threat occurs when an external user somehow gains access to a system or information they were not supposed to be able to see. An example could be a Web-based application that asks for an ID number and returns personal information on an individual without authenticating the user’s identity. One author of this study, required to provide his Social Security number online to an institution as part of a conference registration process, refused to do so and entered 111-11-1111, only to find that number and similar numbers had been taken. In frustration, he then put in a random number that accidentally matched a real number in the system, which in turn caused the system to provide all kinds of personal information about an earlier subscriber. Notified of the system design failure, the institution, quickly and with appreciation, fixed the system. The primary tools for defending against such exposure are policies and procedures, especially those that incorporate security into system design and testing, along with awareness and training activities geared toward ensuring that confidential information is not left exposed to unintended users.

**Internal and intentional.** Intentional attacks from internal users are not uncommon and could occur for reasons including personal gain, revenge against a perceived wrong by a colleague, supervisor, or professor, or just the thrill of doing it. IT security technologies such as internal firewalls, strong authentication mechanisms, data encryption, and intrusion detection tools can help the institution protect against such threats. Additionally, criminal background checks of employees with access to sensitive information, clear mechanisms for IT security policy enforcement, and physical security around key systems can help the institution protect itself against such threats.

**External and intentional.** Most people think of this attack type when they hear about an IT security breach: a willful attack by an external hacker. Again, IT security technologies such as perimeter and internal firewalls, strong authentication mechanisms, data encryption, and intrusion detection tools can help protect the institution against such threats. Likewise, policies and procedures that focus on detecting and reacting to external threats, cooperating with law enforcement, and removing compromised systems from the institution’s network are important tools against such threats, as are user awareness and training.

This model helps demonstrate the need for an IT security approach that balances security’s technological and cultural aspects. It shows, for example, that technology can help protect against intentional threats but is less effective against accidental ones. Similarly, cultural tools such as policies, procedures, and awareness provide a strong defense against accidental exposures and complement technology to provide a stronger defense against intentional threats.

**Developing a Business Case for IT Security**

Institutions can develop a business case for IT security using a simple model, such
as Figure 10-3. This model profiles and compares risks and effectively presents them to nontechnical management. One axis represents the perceived risk to the institution, which could include factors such as the number of times the risk has been observed, defense mechanisms currently in place to defend against that risk, and potential damage (both financial and otherwise) to the institution should the risk become reality. The second axis, implementation difficulty, could encompass cost and level of staff effort to implement a solution, along with the cultural resistance a solution might face.

Ranking potential IT security initiatives in this way yields four major categories.

*Discretionary improvements* are easy to implement but address low-risk issues. Institutions may choose to implement these recommendations over time, on the basis of resource availability.

*Low-value initiatives* are difficult to implement and address a low-risk issue. For such initiatives, institutions might conduct additional analysis to determine whether the effort necessary is worthwhile, given the low incremental benefit it provides. Institutions may also wish to defer the implementation of these initiatives until a later date, or choose not to implement them at all.

*Quick wins* address high-risk areas and would not be difficult to implement. Institutions would likely want to implement solutions for all risks that fall into this category as quickly as possible.

*Necessary projects* address a high-risk area but require a high level of effort to implement. Because they are probably necessary to implement, their difficulty means they need to be treated as distinct projects. Institutions may wish to further prioritize the implementation of initiatives in this category by balancing the risk’s immediacy against the availability of resources to correct the issue.

<table>
<thead>
<tr>
<th>Implementation Difficulty</th>
<th>Risk to Institution</th>
<th>Discretionary Improvements</th>
<th>Low Value</th>
<th>Quick Wins</th>
<th>Necessary Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 10-3. IT Security Risk Analysis Framework*
The Changing IT Security Environment

The IT security arena has been the Wild West of the information technology field for the last decade. Since the explosion in Internet usage in the mid-1990s, the IT security field has changed rapidly, moving faster than the legal environment, technology vendors, and many IT practitioners themselves have been able to react. However, in the past several years, the environment itself has started to change, both for better and worse. Terry Gray captured some of these changes and their ramifications in his provocative presentation, discussed earlier. Among the changes he noted were greater reliance on self-imposed denial-of-service, firewalls everywhere, more tunneled traffic through fewer ports, and more difficult troubleshooting.

The legal system has begun to understand cyber crime and is starting to define what constitutes a crime in the online world and to set real penalties for malefactors. However, as with anything new, some feel that the emerging laws have swung the pendulum too far in the other direction and that the laws will require some tweaking to be administrable and effective.

Technology vendors are beginning to understand that security is an important part of their product offerings. Some have begun to integrate security into their products, although there is still a long way to go, particularly for vendors of desktop operating systems. Indeed, vendors could and should use higher education’s needs and open environment as a testing ground as they continue to develop products for broad end-user application. In many ways, the higher education environment mirrors the world of most private Internet users.

And IT professionals have also begun to change, with IT security officers becoming members of a distinct profession with its own certifications, toolsets, and responsibilities. However, even as the IT security area matures, one thing will likely stay the same for some time to come: rapid change.

Technology

IT security technologies have changed significantly since the early days of IT security. Whereas higher education IT security visionaries once had to develop their own tools to secure their systems (for example, MIT’s creation of the Kerberos authentication toolset in the 1980s), today IT security professionals have a wide variety of tools available from a huge number of vendors and the open-source community. These tools’ sophistication continues to increase, as does their ease of use, bringing more powerful capabilities to institutions without large IT departments.

Institutions must continue to take advantage of IT security technologies’ new capabilities because, as with any arms race, the tools available to the hacker community are also evolving rapidly. This will likely increase the pool of potential attackers because the availability of automated, freely distributed tools that exploit known vulnerabilities in commonly deployed operating systems and applications brings ever greater capabilities to hackers who need increasingly less knowledge to operate these tools. Bruce Judd, associate vice president for university computing and telecommunications at San Jose State University, succinctly described this challenge: “This is a cat-and-mouse game. Hackers are always getting better, as are my tools to deal with them.”

Legal Environment

As the legal system begins to catch up with the advances of the Internet Age, new legislation will likely help IT security manage-
ment in the long term, although it is creating near-term headaches for many institutions.

At the federal level, laws like HIPAA and FERPA (the Family Educational Rights and Privacy Act) change the IT security equation for many institutions. Both of these laws contain specific provisions governing the privacy of certain types of data and, in the case of HIPAA, contain specific rules for IT security at institutions dealing with health-care data. Both laws up the ante for compliance with IT security provisions as well, and large fines and jail time are possible for violations. In addition to these federal regulations, some states, such as California, are also passing IT security legislation.

The legal environment promises to get more complex as new initiatives around homeland security, identity theft, spam e-mail, and other hot issues will likely continue to impose new requirements on IT security professionals. As some health-care organizations have done in response to HIPAA, institutions may be able to turn legislation-mandated changes into an opportunity to revamp their IT security capabilities and community practices, rather than trying to meet the requirements with their existing IT security architectures and policies. John Houston, privacy officer and director of IS for the University of Pittsburgh Medical Center, said, "A lot of what they are telling us to do under the [HIPAA] security rule are really things we needed to do anyway."

Another issue institutions need to face is that the reasons for attacks also may be changing. In the past, many hackers who broke into university computer systems did so just because they could or because they wanted access to the system to use it to attack another system. Today's attackers seem to have more-nefarious plans: they attempt to use worms or other means to take control of large numbers of computers and then use them to launch distributed denial-of-service attacks against other entities. For example, in August 2003, hackers compromised at least 2,400 computers at Stanford University by exploiting a known (and patchable) hole in the Windows operating system. Although the infection was discovered before the machines were used to attack other systems, it still cost the university significant time and effort to clean and patch all of the machines. Identify theft is also causing growing concern, and universities may be increasingly targeted because they hold personal data for large numbers of students and employees.

**Future Trends**

It is impossible to accurately predict the future, and given the rapid changes in the IT security space, it would be foolish to try to prognosticate about tactical-level changes institutions will face in the coming years. However, from our research and interviews, we were able to discern some higher-level trends.
Technology Trends

In Chapter 4, we profiled the technologies institutions have already installed and their plans for future deployments. When analyzing this data, several trends emerge. First, institutions as a whole continue to implement core security technologies, such as SSL for Web transactions and perimeter firewalls. More than 70 percent of our respondents have such technologies in place today, and within one year, 88 percent plan to have implemented these technologies, with the numbers going above 92 percent within two years. Second, institutions plan to accelerate the pace of implementing more advanced security technologies. For example, only 48 percent of institutions reported having an enterprise directory in place at the time they were surveyed, but 86 percent plan to have such a system in place within one year, and 94 percent within two years. Other rapidly growing technologies include intrusion prevention and detection tools, encryption, and VPNs, the use of which will grow at nearly a 40 percent pace over the next year.

Finally, planned use of emerging security technologies seems to be more measured. For example, only 1 percent of institutions were using technologies like Shibboleth or biometric authentication at the time of our survey. Within one year, 17 percent of institutions plan to be using Shibboleth, and 6 percent plan to be using biometrics; within two years, the figures rise to 41 percent for Shibboleth and 24 percent for biometrics. These growth rates suggest that higher education is cautious about implementing new technologies, although institutions do recognize the need and plan to use them in the future.

As institutions continue down the path of implementing many traditional security technologies, the world of IT security continues to evolve rapidly, with both the sophistication of threats and the power of tools designed to combat them increasing quickly. In such a rapidly changing environment, there is some concern that traditional security technologies might need to yield to new paradigms for keeping organizations secure. Ken Klingenstein espoused the viewpoint that “newer [IT security] technologies may not be a fit with older designs.”

One such paradigm shift is the increasing use of middleware—software that facilitates interactions between disparate computer systems—to deal with the ever-increasing complexity of relationships between systems, individuals, and organizations. Examples of middleware IT security solutions include enterprise directories, which can pass one set of authentication credentials for a user to multiple systems within an institution’s network; role-based security for authorization, which provides users access to certain applications and data in multiple systems on the basis of their role(s) in the organization; and Shibboleth, a new open-source technology that allows cross-organizational sharing of attributes about users.

Increased Accountability

IT security is quickly moving from an issue relevant only to technologists to an everyday concern for people in all walks of life. Issues such as identity theft are becoming fixtures on the nightly news, and efforts to combat music piracy, spam, and other nuisances and new cyber crimes make headlines every day. As a result, institutions will be under increased pressure from their constituents to provide robust IT security as awareness of its importance rises.

University students and employees will not be the only ones to notice IT security’s increased importance. Politicians at both the federal and state levels have begun to tackle IT security issues, and, as we discussed earlier in this chapter, new laws with real penalties
for violations are emerging that will force institutions to rethink their approach to IT security management. Finally, pressure will likely emerge from institutional business partners. For example, credit card companies require that organizations accepting their cards provide minimum levels of security. Similar expectations could increase from other key partners, including grantors of financial aid and research dollars.

In this environment, experiencing an IT security failure will do more than give the institution a short-lived black eye. Emerging legislation provides for stiff fines and possible jail time for violators, and it is probably only a matter of time before civil litigation for personal information exposure becomes rampant. While this environment will require all organizations, including universities, to improve their IT security environments, the increasing accountability will also likely make IT security more of an executive-level concern, making it easier for IT security managers to obtain the resources they need to make these improvements.

Centralization and Standardization

As the complexity of security issues and technologies grows, and as the time available to deal with threats decreases because of the automated nature of many new attacks, individual departments and research labs within institutions will in many cases have neither the funding nor the expertise to maintain their own IT security. This, in turn, may precipitate a move to more standardized and centralized IT security management at large institutions. Likewise, at some institutions, the increased spotlight on IT security may result in a mandate from senior management to consolidate IT security operations in a professional IT security organization to reduce the institution’s risk exposure.

Some institutions have already begun to offer centralized IT security management services to their communities, although their use is not mandated at this point. For example, the University of Michigan has begun to implement a centrally managed logical firewall system. Paul Howell, information systems security officer, explained, “I have been working closely with some of the network engineers on campus. We have come up with a technical solution that creates the appearance of a firewall—a logical firewall. We are working with several novel firewall products. We are able to give the illusion to a group that they have a firewall dedicated to them and that they administer [it] and no one else can fuss with it; no one else can see the policy and the logs. But in actuality they are operating a virtual firewall that exists on a shared resource that is hosting many firewalls—like a single machine that hosts a half-dozen Web domains.”

At San Jose State University we found another example of a centrally managed service designed to improve security. As part of its recent enterprise resource planning system implementation, the institution was left with an underutilized mainframe system. Rather than decommission the system, in partnership with IBM they reconfigured the mainframe to provide virtual Linux servers to the campus. Bruce Judd said, “We are the first university to provide those in a large scale to individual faculty at no cost.” In addition to these virtual Linux servers, Judd’s team has provided an Oracle database site license and assorted open-source applications. As a result, they hope to convince faculty members to use this professionally managed system rather than setting up and maintaining their own teaching and research systems.

Sharing the Burden

As the demand for IT security continues to grow, many institutions, especially smaller
ones, may find themselves overwhelmed by the level of resources needed to keep up. As a result, we anticipate that smaller institutions may turn outside for a solution. One answer may be to collaborate with other small institutions, forming partnerships or consortia to develop shared IT security management capabilities. Martin Smith, chief information officer at Embry-Riddle Aeronautical University, expressed this view. “Schools are going to form consortia. We are talking with some of our local schools about forming a consortium to deal with security and disaster backup. No school can afford to do it themselves, with money and budgets tight in the state and private schools.” Another alternative may be to turn to managed security services vendors to handle the bulk of day-to-day IT security management.

While some institutions are looking to collaborate on developing IT security management capabilities, others are coming together to develop new IT security solutions. For example, several major research universities are jointly sponsoring Shibboleth, a toolset designed to let institutions share access controls for Web resources. We expect such efforts to continue as institutions try to develop solutions to some of higher education’s IT security needs.

**Conclusion**

This study’s quantitative and qualitative data suggest that many higher education institutions provide levels of IT security that are roughly on par with their counterparts in the corporate world, despite a perceived lack of resources and some unique differences and challenges they face. However, the data indicated that some institutions still have a long way to go in providing high-quality IT security services.

Our results also indicate that while many institutions have implemented a range of technologies to combat IT security threats, far fewer use awareness programs and the acceptance of comprehensive IT security policies and procedures to resolve cultural issues that impact IT security. And somewhat surprisingly, IT security does not appear to be an executive-level issue at many institutions.

Colleges and universities face some significant challenges in implementing IT security, including resource constraints, ever-increasing threats, a changing legal landscape, and rapid technology advancements. And while universities and colleges must undergo some degree of change to overcome these obstacles, our data indicate that the higher education community is rising above these challenges and providing a secure teaching, research, and business environment for its constituents.

**Endnotes**


Appendix A
Interviewees in Qualitative Research

Austin Community College
William Carter, Associate Vice President of Information Technology

Embry-Riddle Aeronautical University
Howard Muffler, Chief Security Officer
Martin Smith, Chief Information Officer
Taryn Wiskirchen, University Risk Manager

Emory University
Randy Conyers, External Auditor, Deloitte & Touche
Peter Day, Emerging Technologies Specialist
Jay Flanagan, Security, Team Lead, ITD Technical Services
Don Harris, Vice Provost for Information Technology and Chief Information Officer
William Mulcahey, Chief Audit Officer

Florida Memorial College
Winston Akin-Cole, Senior Systems Programmer
Peter Bonasto, Vice President for Information Management and Technology
Pam Scriven, Director of Information Technology

Georgia Institute of Technology
Robert N. Clark, Jr., Director of Internal Auditing
John Mullin, Associate Vice Provost, Associate Vice President, and Chief Information Officer for Information Technology
Georgia State University
Mary Jane Casto, Interim Associate Provost and Chief Information Officer
Martin Fraser, Professor and Chair, Computer Science Department
Susan Mondello, Internal Audit
William Paraska, Director of University Computing and Communications Systems

Indiana University
Mark Bruhn, Chief IT Security and Policy Officer and Associate Director of the IU Center on Applied Cybersecurity Research
Beth Cate, Associate University Counsel
Eric D. Cosens, Information Systems Auditor
Tom Davis, University IT Security Officer
Michael Egolf, Manager of Enterprise Systems Administration
Merri Beth Lavagnino, Deputy IT Policy Officer
Michael McRobbie, Vice President for Information Technology, Chief Information Officer, and Vice President of Research
Clark Sorensen, Manager of Information Systems and Services and Senior Assistant Registrar

Maricopa Community Colleges
Carol Myers, Director, ITS Security Services
John Schroeder, Director of Infrastructure and Operations
Ruth Unks, Director of Risk Management

Massachusetts Institute of Technology
Michail Bletsas, Director of Computing, MIT Media Lab
James Bruce, Vice President for Information Systems
John Curry, Executive Vice President
Robert Mahoney, Team Leader, Network Security
Timothy McGovern, Senior Project Manager of Stop-It
Jeffrey Schiller, Network Manager

Mayville State University
Keith Stenehjem, Chief Information Officer

North Dakota University System
Dick Jacobson, NDUS IT Security Officer

San Jose State University
Bruce Judd, Associate Vice President, University Computing and Telecommunications
South Dakota State University
   Michael Adelaine, Chief Information Technology Officer
   Andrew Conley, Network Security Officer
   Dennis Todey, South Dakota Extension/State Climatologist

The University of Texas at Austin
   Dan Updegrove, Vice President for Information Technology

University of California, Berkeley
   Jack McCredie, Chief Information Officer and Associate Vice Chancellor

University of Chicago
   Gregory Jackson, Vice President and Chief Information Officer
   Larry Lidz, Senior Network Security Officer

University of Michigan
   Elizabeth Sweet, Director of User Advocacy
   Paul Howell, Information Systems Security Officer

University of Montana
   Ray Ford, Vice President for Information Technology

University of Notre Dame
   Gary Dobbins, Director, Information Security
   Gordon Wishon, Chief Information Officer, Associate Vice President, and
   Associate Provost

University of Washington
   Kirk C. Bailey, Manager, Strategic Computer Security Services, Computing
   and Communications
   Scott F. Barker, Senior Lecturer and Director, Information Technology,
   The Information School
   Elizabeth A. Cherry, Director, Risk Management
   Terence E. Gray, Director, Networks and Distributed Systems, Computing and
   Communications
   Michael S. Hornung, Security Operations, Computing and Communications
   Weldon E. Ihrig, Executive Vice President
   Ronald A. Johnson, Vice President, Computing and Communications
   Edward M. Lightfoot, Director, Information Systems, Computing and Communications
   R. L. "Bob" Morgan, Senior Technology Architect, Computing and Communications
   Sandra S. Moy, Director, University Computing Services, Computing and
   Communications
   Oren Sreebny, Assistant Director, Client Services, Computing and Communications
University of Wisconsin–Madison
  Kim Milford, Information Security Manager
  Jeffrey Savoy, Information Security Officer

Yale University
  Douglas Kankel, Professor of Molecular, Cellular, and Developmental Biology
  Morrow Long, Director, Information Security
  Philip Long, Chief Information Officer
  Salvatore Rubano, Deputy Director, University Audit
Appendix B
Institutional Respondents to the Online Survey

Agnes Scott College
Algonquin College
Angelo State University
Anne Arundel Community College
Appalachian State University
Aquinas College
Arizona State University
Arizona State University West
Arkansas State University Newport
Athabasca University
Auburn University
Austin Community College
Azusa Pacific University
Ball State University
The Banff Center
Barnard College
Bastyr University
Baylor University
Bellarmine University
Bemidji State University
Berea College
Berklee College of Music
Bethune-Cookman College
Big Bend Community College
Biola University
Brandeis University
Brenau University
Bridgewater State College
British Columbia Institute of Technology
Bronx Community College/CUNY
Brooklyn Law School
Broome Community College
Brown University
Bryant College
Bucknell University
Caldwell College
California Maritime Academy
California Polytechnic State University
San Luis Obispo
California State University–Hayward
California State University, Office of the Chancellor
California State University–Bakersfield
California State University–Northridge
California State University–San Marcos
California State University–Stanislaus
Calvin College
Camosun College
Canisius College
Catawba College
Cedar Crest College
Cedarville University
Central College
Central Connecticut State University
Central Missouri State University
Central State University
Central Washington University
Chandler-Gilbert Community College
<table>
<thead>
<tr>
<th>College Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charleston Southern University</td>
</tr>
<tr>
<td>Chatham College</td>
</tr>
<tr>
<td>Cheyney University of Pennsylvania</td>
</tr>
<tr>
<td>City University of New York</td>
</tr>
<tr>
<td>Claremont Graduate University</td>
</tr>
<tr>
<td>Clarke College</td>
</tr>
<tr>
<td>Clayton College and State University</td>
</tr>
<tr>
<td>Cleveland Institute of Art</td>
</tr>
<tr>
<td>Clovis Community College</td>
</tr>
<tr>
<td>Coastal Carolina Community College</td>
</tr>
<tr>
<td>Colby-Sawyer College</td>
</tr>
<tr>
<td>Colgate University</td>
</tr>
<tr>
<td>College for Lifelong Learning</td>
</tr>
<tr>
<td>College Misericordia</td>
</tr>
<tr>
<td>College of Saint Catherine</td>
</tr>
<tr>
<td>College of the Holy Cross</td>
</tr>
<tr>
<td>College of the Menominee Nation</td>
</tr>
<tr>
<td>The College of New Jersey</td>
</tr>
<tr>
<td>The College of Saint Scholastica</td>
</tr>
<tr>
<td>Collin County Community College</td>
</tr>
<tr>
<td>Colorado School of Mines</td>
</tr>
<tr>
<td>Columbia University</td>
</tr>
<tr>
<td>Concordia Theological Seminary</td>
</tr>
<tr>
<td>Concordia University, Portland</td>
</tr>
<tr>
<td>Connecticut College</td>
</tr>
<tr>
<td>Coppin State College</td>
</tr>
<tr>
<td>Cornell University</td>
</tr>
<tr>
<td>County College of Morris</td>
</tr>
<tr>
<td>Crown College</td>
</tr>
<tr>
<td>Crownpoint Institute of Technology</td>
</tr>
<tr>
<td>Cuyahoga Community College</td>
</tr>
<tr>
<td>Dakota Wesleyan University</td>
</tr>
<tr>
<td>Davenport University</td>
</tr>
<tr>
<td>Davidson College</td>
</tr>
<tr>
<td>Davis &amp; Elkins College</td>
</tr>
<tr>
<td>Denison University</td>
</tr>
<tr>
<td>Douglas College</td>
</tr>
<tr>
<td>Eastern Michigan University</td>
</tr>
<tr>
<td>Eastern Oregon University</td>
</tr>
<tr>
<td>Eastern Washington University</td>
</tr>
<tr>
<td>Eckerd College</td>
</tr>
<tr>
<td>Edmonds Community College</td>
</tr>
<tr>
<td>Elizabethtown College</td>
</tr>
<tr>
<td>Elmhurst College</td>
</tr>
<tr>
<td>Embry-Riddle Aeronautical University</td>
</tr>
<tr>
<td>Emory University</td>
</tr>
<tr>
<td>Fairfield University</td>
</tr>
<tr>
<td>Fairmont State College</td>
</tr>
<tr>
<td>Fayetteville State University</td>
</tr>
<tr>
<td>Fielding Graduate Institute</td>
</tr>
<tr>
<td>Florida Atlantic University</td>
</tr>
<tr>
<td>Florida Memorial College</td>
</tr>
<tr>
<td>Florida State University</td>
</tr>
<tr>
<td>Foothill-DeAnza Community College</td>
</tr>
<tr>
<td>District</td>
</tr>
<tr>
<td>Fort Belknap College</td>
</tr>
<tr>
<td>Francis Marion University</td>
</tr>
<tr>
<td>Franklin and Marshall College</td>
</tr>
<tr>
<td>Franklin W. Olin College of Engineering</td>
</tr>
<tr>
<td>Frederick Community College</td>
</tr>
<tr>
<td>Frostburg State University</td>
</tr>
<tr>
<td>Furman University</td>
</tr>
<tr>
<td>Gallaudet University</td>
</tr>
<tr>
<td>Geneseec Community College</td>
</tr>
<tr>
<td>Georgetown University</td>
</tr>
<tr>
<td>The George Washington University</td>
</tr>
<tr>
<td>Georgia College &amp; State University</td>
</tr>
<tr>
<td>Georgia Perimeter College</td>
</tr>
<tr>
<td>Georgia State University</td>
</tr>
<tr>
<td>Gettysburg College</td>
</tr>
<tr>
<td>Glendale Community College (AZ)</td>
</tr>
<tr>
<td>Glendale Community College (CA)</td>
</tr>
<tr>
<td>Greenbrier Community College Center</td>
</tr>
<tr>
<td>Guilford College</td>
</tr>
<tr>
<td>Hamilton College</td>
</tr>
<tr>
<td>Harford Community College</td>
</tr>
<tr>
<td>Harvard University</td>
</tr>
<tr>
<td>Heidelberg College</td>
</tr>
<tr>
<td>Hiwassee College</td>
</tr>
<tr>
<td>Hofstra University</td>
</tr>
<tr>
<td>Hollins University</td>
</tr>
<tr>
<td>Houston Community College System</td>
</tr>
</tbody>
</table>
| Humber College Institute of Technolo-
|    gy and Advanced Learning          |
| Humboldt State University            |
| Illinois College                     |
| Illinois Institute of Technology     |
| Illinois Wesleyan University         |
| Immaculata University                |
Northern Illinois University
Northern Kentucky University
Northern Michigan University
Northwest Missouri State University
Northwestern College of Iowa
Norwich University
Oakland University
Oberlin College
Ohio Dominican University
Ohio Northern University
The Ohio State University
Oklahoma State University
Oklahoma State University–Tulsa
Onondaga Community College
Oregon State University
Otterbein College
Our Lady of the Lake University
Pace University
Pierce College
Pennsylvania College of Technology
The Pennsylvania State University
Pensacola Junior College
Philander Smith College
Phillips Academy
Phoenix College
Pima County Community College
Pomona College
Portland State University
Prince George's Community College
Princeton University
Providence College
Purchase College, SUNY
Quinnipiac University
Raritan Valley Community College
Rensselaer Polytechnic Institute
Rhode Island School of Design
Rice University
Ringling School of Art and Design
Rio Salado College
Roane State Community College
Ryerson University
Saddleback College
Saint Bonaventure University
Saint John's University/College of Saint Benedict
Saint Mary's University of Minnesota
Salem State College
Sam Houston State University
San Diego State University
Saskatchewan Institute of Applied Science & Technology
Savannah College of Art and Design
The School for Film and Television
School of the Art Institute of Chicago
Scottsdale Community College
Seton Hall University
Shenandoah Community College
Siena College
Siena Heights University
Sinclair Community College
South Dakota School of Mines & Technology
South Dakota State University
Southern Methodist University
Southwest Texas State University
Southwestern Indian Polytechnic Institute
Southwestern University
Spring Hill College
St. Cloud State University
St. Mary's College of Maryland
St. Olaf College
St. Petersburg College
St. Philip's College
Stanford University
SUNY College at Plattsburgh
SUNY College of Environmental Science & Forestry
SUNY College of Optometry
SUNY College of Technology at Cobleskill
SUNY System Administration
Swarthmore College
Sweet Briar College
Syracuse University
Temple University
Tennessee Board of Regents
Texas A&M University at Galveston
Texas Christian University
Texas State Technical College–Harlingen
Texas State Technical College–West Texas, Sweetwater
Trinity University
Troy State University
Troy State University Montgomery
Ulster County Community College
United States Military Academy
University at Albany, SUNY
University at Buffalo, SUNY
University College of the Fraser Valley
University of Alabama
University of Alabama in Huntsville
University of Alaska Anchorage
University of Alaska Fairbanks
University of Alaska Statewide System
University of Arizona
The University of British Columbia
University of Calgary
University of California, Berkeley
University of California, Irvine
University of California, Los Angeles
University of California, Merced
University of California, Office of the President
University of California, San Diego
University of California, San Francisco
University of California, Santa Cruz
University of Central Florida
University of Chicago
University of Colorado at Denver
University of Delaware
University of Detroit Mercy
University of Florida
University of Guelph
University of Hawaii at Manoa
University of Houston
University of Houston–Clear Lake
University of Illinois at Chicago
University of Illinois at Springfield
University of Illinois at Urbana-Champaign
The University of Iowa
University of Kansas
The University of Kansas Medical Center
University of Kentucky
University of La Verne
University of Maine at Presque Isle
University of Manitoba
University of Maryland, Baltimore County
University of Massachusetts
The University of Memphis
University of Miami
University of Michigan–Ann Arbor
University of Michigan–Dearborn
University of Minnesota, Duluth
University of Minnesota, Twin Cities
University of Missouri–Kansas City
University of Nebraska–Lincoln
University of Nebraska at Omaha
University of Nebraska Central Administration
University of New Brunswick
University of New Hampshire
University of New Mexico
University of North Carolina at Chapel Hill
University of North Carolina at Charlotte
University of North Carolina at Greensboro
University of North Carolina, Office of the President
University of North Dakota
University of North Florida
University of North Texas HSC at Fort Worth
University of Notre Dame
University of Oklahoma
University of Oklahoma Health Sciences Center
University of Oregon
University of Pennsylvania
University of Puget Sound
University of Rhode Island
University of Richmond
University of Rochester
University of Saint Francis
University of Saint Thomas
University of Scranton
University of South Carolina
University of South Carolina–Salkehatche
The University of South Dakota
University of South Florida
The University of Tennessee
University of Tennessee at Chattanooga
The University of Texas at Arlington
University of Texas at Dallas
University of Texas at San Antonio
University of Texas Medical Branch
University of the District of Columbia
University of the Incarnate Word
University of the Pacific
University of the Sciences in Philadelphia
University of the Virgin Islands
The University of Toledo
University of Tulsa
University of Utah
University of Washington
University of Washington, Bothell
University of Waterloo
University of West Florida
University of Winnipeg
University of Wisconsin–Eau Claire
University of Wisconsin–Madison
University of Wisconsin–Platteville
Valencia Community College
Vancouver Community College
Vassar College
Vermont Law School
Washington College
Washington University in St. Louis
Weber State University
Wellesley College
West Chester University of Pennsylvania
West Virginia Wesleyan College
Western Carolina University
Western Michigan University
Westminster College
Wheaton College
Whitman College
Whittier College
Wichita State University
Widener University
William Woods University
Williams College
Yale University
Appendix C
Glossary

-A-

Access: The ability to enter a secured area, either physically or virtually.
Access control: A set of procedures and processes performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and limit access to the resources of a system to only authorized persons, programs, processes, or other systems.
AES (advanced encryption standard): A relatively new encryption standard used by the U.S. federal government for unclassified information. It is freely available for worldwide use.
Antivirus: Software used to prevent infection of computers by computer viruses and worms and to remove such infections after they occur.
Audit: An independent review and examination of system records and activities to access their veracity and completeness.
Audit trail: A set of records that provides documentary evidence of processing. It is often a chronological record of when users log in, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred.
Authenticate/Authentication: A method for confirming a user’s identification, often as a prerequisite to allowing access to resources in a system.
Authenticated user: A user who has accessed a computer system with a valid identifier and authentication combination.
Authenticity: The ability of a third party to verify that the content of a message has not been modified in transit.
Authorization: The privileges and permissions granted to an individual by a designated official to access or use a program, process, information, or system.

-B-

Backup: A copy of a program or data file for the purposes of protecting against loss if the original data becomes unavailable.
Biometrics: The identification of a user (and possibly access control) based on a physical, unchangeable characteristic, such as a fingerprint, iris, face, voice, or handwriting.
Breach: A successful attack on an organization’s computing resources, resulting in penetration of one or more secured systems or applications. A breach does not necessarily imply that theft or damage has occurred—simply that an attacker was able to access the system.


Challenge/response: A security procedure in which one communicator requests authentication of another communicator, and the latter replies with a pre-established appropriate reply.


Compromise: The disclosure of sensitive information to persons not authorized for access or having a “need to know.”

Confidentiality: Protection of information from unauthorized use or disclosure.

Content filtering: A system that blocks certain content, such as objectionable Web pages, spam e-mail, or music files, preventing them from being accessed by users.

Cryptography: A coding method, using an algorithm, by which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format) to ensure the secrecy and/or authenticity of data.

Data integrity: The state that exists when computerized data are the same as those that are in the source documents and have not been exposed to accidental or malicious alterations or destruction.

Denial of service (DoS): The inability of a computer system to perform its designated mission. A denial of service includes the prevention of authorized access to resources or the delaying of time-critical operations.

Denial-of-service attack: An attack in which a mail or Web server is purposely overloaded with fake requests so that it cannot respond properly to valid ones.

Designated security officer: The person responsible for ensuring that security is provided for and implemented throughout the life cycle of the computer system.

DHCP (dynamic host configuration protocol): A common method of assigning IP addresses to network devices without requiring a permanent IP address for each device. Addresses are assigned to a device as it appears on the network and are released and available for reuse when the device is removed.

Digital certificate: The electronic equivalent of an ID card, which works in conjunction with public key encryption to sign digital signatures.

Disaster-recovery plan: A documented, organized process for implementing emergency response, back-up operations, and post-disaster recovery. The plan is maintained to ensure the availability of critical assets (resources) and facilitate the continuity of operations in an emergency.
Distributed denial-of-service attack (DDoS): A denial-of-service attack in which the attackers load their malignant code onto a host of other machines and use them to overload other systems.


DNS (Domain Name System): A service that translates Internet domain names to IP addresses, allowing users to request a connection to a server with an English, rather than a numeric, identifier.

EAP (extensible authentication protocol): A standard for wireless security that allows security authentication data to be passed among RADIUS, the wireless access point, and the wireless client.

Electronic signature: A method and tools used to authenticate the identity of the sender of a message, or to ensure the integrity of the content of the message. Electronic signatures use public key encryption techniques to create a verifiable signature for each document signed. Use of electronic signatures was legalized at the federal level by the Electronic Signatures in Global and National Commerce Act of 2000.

Electronic Signatures In Global and National Commerce Act: U.S. Federal law passed in 2000, stating that electronic signatures may be legally binding for contracts and transactions. Electronic signatures may include digital signatures, click-through agreements at Web sites, biometrics, or digitized versions of handwritten signatures. Many states have passed similar laws.

Encryption: The conversion of text or data into unintelligible (coded) form by means of a reversible translation that is based on a translation table or algorithm.

Enterprise directory: A system for centrally organizing information about an organization’s users, passwords, and authorizations to access networked resources.


Firewall: A system or combination of systems that enforces a boundary between two or more networks. It is a method of guarding a private network by analyzing the data leaving and entering. A firewall generally possesses the following properties: 1) all traffic from inside to outside, and from outside to inside, must pass through it; 2) only authorized traffic, as defined by the firewall’s administrator, is allowed to pass through it; 3) the system itself is immune to penetration.

Firewall, interior: Use of firewall technology to create a barrier between a portion of an internal network and the rest of the internal network.
**Firewall, perimeter:** Use of firewall technology to create a barrier between an organization’s enterprise network and outside networks, such as the Internet.

**Firewall, personal:** A firewall, generally software based, designed to protect one system from attack. A software-based personal firewall is loaded onto the computer it will protect, much as antivirus software is, rather than residing in a separate piece of hardware like larger network firewalls.

---

**GIAC (Global Information Assurance Certification):** A common IT security certification developed and maintained by GIAC, an organization founded by the SANS Institute, a leading resource for IT security professionals. More information can be found at [http://www.giac.org/](http://www.giac.org/).

**Gramm-Leach-Bliley Act of 1999:** This act of Congress requires higher education to notify people they deal with of their right to keep their financial information confidential and to protect their financial data. Protection involves having a plan or security policy that includes designating an employee to coordinate information security, identify and repair weaknesses in computer systems, continually monitor systems, provide security training for employees, and require service providers to comply with the law through contract language requiring compliance. More information can be found at [http://www.senate.gov/~banking/conf/](http://www.senate.gov/~banking/conf/).

---

**Hacker:** A name for an unauthorized person who breaks into or attempts to break into a computer system to which he is not entitled entry by circumventing software security safeguards.

**Hardware token:** A security device carried by a user, required to authenticate to the system. Examples could include a dongle attached to a PC’s USB or serial port or a password generator, such as RSA’s SecureID product. Such devices are often used in conjunction with a password, resulting in two-factor authentication.

**HIPAA (Health Insurance Portability and Accountability Act):** A multifaceted U.S. law passed in 1996. In an information security context, the law sets standards for information security and privacy for organizations dealing with patient-identifiable medical data, as well as penalties for noncompliance. More information about HIPAA can be found at [http://www.hipaa.org/](http://www.hipaa.org/).

**Host:** Sometimes used as a synonym for “server.”

---

**ICMP (Internet control message protocol):** A message control and error-reporting protocol used for communication between servers and Internet gateways. A vulnerability in ICMP results in a type of denial-of-service attack called the “Ping of Death.”

**Information security:** The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

**Information security officer (ISO):** The person responsible for ensuring that security is provided for and implemented throughout the life cycle of the computer system.
Insider attack: An attack originating from inside a protected network, generally by an authorized user of that network.

Integrity: Ensures that 1) data is a proper representation of information, 2) data retains its accuracy, 3) data remains in perfect condition, and 4) the computerized data represent those in the source documents and have not been exposed to accidental or malicious alteration or destruction.

Intruder: An individual who gains, or attempts to gain, unauthorized access to a computer system or unauthorized privileges on that system.

Intrusion detection system (IDS): A system used to detect break-ins or break-in attempts. KPMG defines network-based intrusion detection as systems that analyze network traffic by looking for known patterns of traffic that might indicate an attack. Host-based intrusion detection systems analyze logs produced by operating systems to identify security-related events.

IP (Internet protocol): The most common protocol currently used to send information across data networks. All traffic on the Internet uses this protocol. Using IP, each system on the network is assigned a unique address in the form xxx.xxx.xxx.xxx, which identifies the source and destination of each packet. Standard IP network packets are not encrypted.

IP spoofing: An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

IRC (Internet relay chat): A system for allowing users to chat across networks, including the Internet.

Kerberos: A secret-key network authentication system used for encryption and authentication. Kerberos was designed to authenticate requests for network resources rather than to authenticate authorship of documents. Kerberos was developed at and continues to be enhanced by MIT. More information can be found at <http://web.mit.edu/kerberos/>.

Logging: The process of storing information about events that occurred on the firewall, network, computer, or application.

Malicious code: Software that is intentionally included in a computer system for an unauthorized purpose.

NetBIOS: A networking protocol supported by Microsoft operating systems, used for communication across a local area network.

Network: A communications medium and all components attached to that medium whose responsibility is the transference of information.

Network infrastructure: The links, routers, and switches that allow hosts to communicate with one another.
Nonrepudiation: Method by which the sender is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data. The origin or receipt of a specific message must be verifiable by a third party.

NTP (network time protocol): A protocol used to synchronize systems’ clock times across a network.

Packet: The unit of data sent across a network during transmission. Files are broken into packets of an efficient size for routing by the sending system and reconstructed at the destination.

Password: A string of characters used to authenticate a user to a system or application.

Password, multilevel: Use of more than one password required to access an information resource. For example, a user may have to log in to the network and then use a different password to access a system on the network. Without both passwords, access cannot be obtained.

Password, multiple use: A password assigned to a user that can be used for an unlimited or specified period of time.

Password, single use: A password that can only be used once. Such passwords are often generated by a hardware token that is synchronized to a server. Single-use passwords remove the danger of a password being compromised during transmission across the network.

Perimeter-based security: The technique of securing a network by controlling access to all entry and exit points of the network.

Personnel security: The procedures established to ensure that all personnel who have access to any sensitive information have all the required authorities or appropriate security authorizations.

Physical security: The application of physical barriers, such as locked doors, and control procedures, such as requiring photo IDs to enter certain areas, as preventative measures or safeguards against threats to resources and information.

Ping: A simple program used on TCP/IP networks to determine if another computer is active on the network. The originating system sends a request, and if active, the pinged computer sends a reply.

Port: A logical connection in TCP/IP networking to connect a client to a service. Port numbers can range from 0 to 65536. Commonly used applications such as HTTP have pre-assigned port numbers (HTTP always uses port 80, for example).

Private key: In encryption, one key (or password) is used to both lock and unlock data.

Privacy: The policies that determine what information is gathered, how it is used, and how customers are informed and involved in this process.

Protocols: Agreed-upon methods of communications used by computers.

Public key encryption (PKI): A coding system in which encryption and decryption are done with public and private keys, allowing users who don’t know each other to send secure or verifiable messages.
RADIUS (remote authentication dial-in user service): A client-server protocol and software that allow remote access servers to communicate with a central server to authenticate users and authorize their access to network resources.

Remote access: The hookup of a remote computing device via communications lines such as ordinary phone lines or wide area networks (WANs) to access network applications and information.

Residual risk: The part of risk remaining after security measures have been implemented.

Risk: The likelihood that a vulnerability will be exploited or that a threat may become harmful.

Risk analysis: The process of identifying an organization’s information resources, existing controls, security risks, and vulnerabilities; determining their magnitude; and identifying areas needing safeguards. It establishes a potential level of damage in dollars and/or other assets.

Risk assessment: An estimate of the harm to business likely to result from a security failure and of the likelihood of such a failure occurring, given the threat environment and the measures in place to prevent a failure.

Risk management: The total process of identifying, measuring, controlling, and eliminating or minimizing uncertain events that may affect system resources.

Rogue program: Any program intended to damage programs or data.

Router: A network device that connects multiple networks and forwards network packets to their destinations, based on a series of algorithms. Routers can be configured to allow or block different types of network traffic.

Scan: Testing of a system to determine whether any known vulnerabilities exist on it.

Security awareness: Activities, materials, and/or training designed to make an organization’s user community knowledgeable about potential security threats and how to combat them.

Security incident: Any event and/or condition that has the potential to impact the security of a system and may result from intentional or unintentional actions.

Security policy: The set of laws, rules, and practices that regulate the acceptable use of computer resources and how an organization manages, protects, and distributes controlled information.

SFTP (Secure File Transfer Protocol): An encrypted version of the commonly used FTP file-transfer tool. SFTP functions are often included as part of SSH (secure shell) software.

Shibboleth: An open-source middleware solution created by Internet2/MACE to allow organizations to exchange information about their users in a secure manner that ensures protection of privacy. The purpose of the exchange is typically to determine if a person using a Web browser has permission to access a target resource based on information such as being a member of an institution or a particular class. More information about Shibboleth can be found at <http://shibboleth.internet2.edu/>.
Single sign on: A product or technology that allows users to authenticate once to a central authentication server and be authorized to use multiple applications and network resources without having to log in separately to each one.

Smart card: A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual and/or other information such as digital cash. A smart card holds its own data and applications and does its own processing.

Sniffer: A network device that views all passing packets, allowing the user to see any unencrypted data, including some user name and password traffic.

Social engineering: An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by someone pretending to be an authorized user who telephones users or operators in an attempt to gain illicit access to systems.

SSH (secure shell): An application that provides an encrypted connection, both for authentication and data transmission, for remote login to a UNIX system.

SSL (secure sockets layer): A protocol, originally developed by Netscape, that creates a secure connection between a client (typically a Web browser), and a server through the use of either 40-bit or 128-bit public key encryption. Web pages protected with SSL usually use the “https” prefix.

Switch: A networking device that takes input from multiple ports and channels data to the specific output port that will take the data toward its destination.

TCP/IP: The common networking protocol used for all Internet traffic. Also commonly referred to as IP, or Internet Protocol.

Timeout: A system feature that terminates a user’s session after a pre-determined period of inactivity, requiring the user to reauthenticate before being able to access the system again.

Trojan horse: A computer program that disguises itself as a beneficial or entertaining program but actually contains additional (hidden) functions that damage a computer or installs code that can counteract security measures and be detrimental to network security.

Trusted computing system: A computer and operating system that employs secure hardware and software measures to allow its use for processing a range of sensitive information and can be verified to implement a given security policy.

Tunneling router: A system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption.

Two-factor authentication: Authentication based on something a user knows, such as a password (factor one), plus something the user has, such as an identification card (factor two). To access a network, the user must have both factors.

User identification: The process, usually through a unique character string, by which a user identifies himself to the system as a valid user.

Verification: Comparing two levels of system specifications and ensuring that information has not been changed in transit or in storage, either intentionally or accidentally.
**Virus:** A self-replicating code segment that causes a copy of itself to be inserted in one or more other programs. The virus usually performs an unwanted function. A program does not need to perform malicious actions to be a virus; it only needs to infect other programs.

**VPN (virtual private network):** A remote access system that is replacing traditional dial-up modem pools. Allows remote users to connect to an Internet service provider (ISP) or a private IP-based network and establish a secure connection with network servers through an encrypted tunnel.

**Vulnerability:** An error or a weakness in the design, implementation, or operation of a system.

**Vulnerability assessment:** A review of a system or systems to identify weaknesses or errors in design, implementation, or operation.

**WAN (wide area network):** A network of local area networks (LANs) that provides communication and services over a geographic area larger than that served by a LAN.

**WEP (wired equivalent privacy):** A protocol used to provide security for wireless LAN connections by encrypting the connection between wireless access points and wireless clients. WEP is part of the IEEE's 802.11b wireless networking standard.

**Worm:** A computer program that replicates itself and sends copies from computer to computer. Upon arrival, the worm may be activated to replicate and spread again. In addition, the worm usually performs an unwanted function.

**Y2K:** An acronym for the Year 2000 Problem that involved three specific issues: two-digit data storage (storing data as 00 instead of 2000), leap-year calculations, and special meanings for dates.

**References**


Electronic Journals


Private and Nonprofit Organization Sites


The CERT Coordination Center (CERT/CC) is a center of Internet security expertise located at the Software Engineering Institute, <http://www.sei.cmu.edu>, a federally funded research and development center operated by Carnegie Mellon University. Information ranges from protecting your system against potential problems to reacting to current problems to predicting future problems. Their work involves handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing information and training to help you improve security at your site. See especially <http://www.cert.org/>, <http://www.cert.org/nav/allpubs.html>, <http://www.cert.org/other_sources/books.html>, and <http://www.cert.org/octave/>.


**University Sites**


UCLA Online Institute for Cyberspace Law and Policy: With the growth and development of cyberspace law as a separate discipline, a dynamic new body of scholarship has emerged. The Online Institute’s Cyberspace Law Bibliography—updated regularly since 1995—provides an overview of recent books and journal articles in this area and includes a growing number of links to the works themselves, <http://www.gseis.ucla.edu/iclp/hp.html>.


**Government Sites**


NIH (National Institutes of Health), <http://www.alw.nih.gov/Security/security.html>, provides a number of articles and links about information technology security.


**Surveys**


Legal Environment: Laws Affecting Security
